UNIVERSIDAD CARLOS III DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

SEGURIDAD LÓGICA Y DE ACCESOS Y SU AUDITORÍA

PROYECTO FIN DE CARRERA

INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN

Autora: Marta Monte de Paz

Director: Miguel Ángel Ramos González

Marzo, 2010

A mi madre por su amor incondicional y su eterna paciencia.

A todas aquellas personas que me han dado ánimos durante la realización de este proyecto.

A mi tutor por la ayuda brindada en estos meses.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

V. CUESTIONARIO

INTRODUCCIÓN

El objetivo de este documento es concienciar a las personas, especialmente a las empresas, de la importancia de la seguridad. Invertir tiempo, esfuerzo y dinero en controles de seguridad asegurará en gran medida la continuidad de un negocio. De forma concreta, este proyecto se centra en la seguridad lógica y de accesos. Además, la realización de auditorías permitirá reflejar qué aspectos pueden mejorarse en una organización.

En el primer capítulo, titulado "*Información*", se expone la importancia de salvaguardar la **información** y las características que debe contemplar una información de calidad. Asimismo, se detalla el uso de sistemas de información que facilitan cuantiosamente las actividades en una entidad.

En el segundo apartado, dedicado a la **seguridad**, se pretende sensibilizar al individuo de la importancia de la seguridad en las empresas. Las organizaciones deben conocer los peligros a las que se enfrentan sus activos, planificando qué bienes desean salvaguardar, de qué y de quiénes, y cómo llevar a cabo esta protección.

"*Seguridad Lógica*" es el título del siguiente capítulo que explora las amenazas lógicas que puede sufrir una empresa. También refleja algunos controles que, utilizados de forma correcta, si no eliminan, al menos, minimizan el impacto causado en la compañía.

El cuarto capítulo está dedicado a la **auditoría.** Realizar auditorías permite identificar los puntos débiles de una organización. En especial, se expone la trascendencia que tienen las auditorías informáticas en las organizaciones.

En el siguiente apartado, se explica una aplicación realizada que contiene un **cuestionario** que podría utilizarse como herramienta en la ayuda de auditoría informática referente a la seguridad lógica y de accesos en las entidades.

A continuación, concurre un breve capítulo que expone las conclusiones obtenidas de este escrito. Finalmente, se muestra un glosario de términos, la bibliografía utilizada y un apartado de "*Anexos*" que exponen una serie de artículos de leyes relacionadas con el tema tratado en este documento y unas tablas referentes al cuestionario realizado.

I. LA INFORMACIÓN

1. 1 Introducción

La información es un conjunto de datos dispuestos de manera que nos permitan adquirir cualquier tipo de conocimiento. Asimismo, es uno de los principales activos de las organizaciones, por lo que salvaguardarla es vital para la continuidad del negocio.

Vivimos en la sociedad de la información y de las telecomunicaciones. La informatización de la información es necesaria para competir en el mercado e incluso para sobrevivir. Antonio Creus expone en su libro "*Fiabilidad y seguridad: su aplicación en procesos industriales*" que el coste de la seguridad informática en una empresa se ubica entre el 4% y el 10% del gasto total informático.

Hemos evolucionado cuantiosamente en los últimos años, gracias a la llegada de los ordenadores. A día de hoy, manejamos grandes volúmenes de información que tratamos, en su mayoría, de forma automática. En consecuencia, las personas pueden tener la percepción de no saber cómo ni dónde se guardan los documentos.

La llegada de Internet trajo consigo una revolución en la sociedad. Ahora es posible encontrar casi cualquier información en la red, la mayoría de forma gratuita. Internet ha revolucionado nuestra forma de comunicarnos. Incluso la comunicación entre empleados ha cambiado y, hoy en día, es bastante probable que aún encontrándose a pocos metros, los trabajadores de una compañía se comuniquen vía *e-mail*. La red abre puertas al conocimiento pero también a posibles peligros de los que se hablará en este documento.

Las empresas deben mentalizarse de que la información conlleva costos. Estos costos están vinculados al almacenamiento, producción y distribución, además de a la seguridad y recuperación de la información. Las organizaciones no deben escatimar en protegerla, sobre todo, la información de carácter personal.

Por otra parte, la información debe ser clasificada según su valor, requerimientos legales y el grado de protección requerido. Generalmente la información deja de ser sensible después de un cierto espacio de tiempo, razón por la cual, tampoco se debe realizar una "sobre-clasificación" que conlleve gastos superfluos.

La información es esencial en la toma de decisiones. Cuanta más calidad tenga la información (completa, exacta y a tiempo), mayor probabilidad habrá de tomar decisiones acertadas. Manejar de forma adecuada la información generada y recibida puede ayudar a lograr una ventaja competitiva en el mercado.

Hoy en día, la información está expuesta a múltiples riesgos y amenazas. Es primordial, por tanto, asegurar la información para el buen funcionamiento de la empresa, involucrando en esta tarea a toda la organización, no solo el Departamento de Seguridad. Sin embargo, es un reto complicado concienciar a todos los empleados de la importancia de la información pero es una labor que la entidad ha de lograr.

1. 2 Marco legal

Hoy en día, debido a la evolución de las nuevas tecnologías, es posible transmitir información de forma conjunta, interrelacionarla, cruzarla… y muchísimas acciones más que dejan fuera de control a la persona titular de esos datos.

Las organizaciones manejan gran cantidad de **datos de carácter personal** que son necesarios para desarrollar su actividad empresarial diaria o de forma publicitaria, identificando posibles clientes de un producto o servicio. En Internet, es sencillo dejar rastro de datos personales, pudiéndose formar incluso, un perfil del usuario sin que éste pueda controlar esa información. Es aquí, donde cobra especial relevancia la protección de datos.

Por este motivo, es ineludible conseguir un equilibrio entre la necesidad que tienen las empresas de gestionar datos de carácter personal y el derecho a la protección de la información.

En España, existe la **Ley Orgánica de Protección de Datos de carácter personal** (LOPD) para regular este tipo de información. El objetivo de la Ley Orgánica 15/1999, de 13 de diciembre, se expone en el Título 1 artículo 1 de dicha ley, detallando que se trata de "*garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*".

Por lo tanto, la LOPD pretende establecer una serie de principios en cuanto al tratamiento de datos de carácter personal y reconoce unos derechos a los titulares de los datos. Asimismo, cabe destacar el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

La LOPD no ha sido la primera sobre esta materia que "ve la luz" en España. En 1992 apareció la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) que regulaba el tratamiento de datos de carácter personal pero sólo de forma automatizada. En el Titulo VI de esta ley ya derogada se creó la Agencia de Protección de Datos regulada en el Real Decreto 428/1993, de 26 de marzo, por el que se aprobó el Estatuto de la **Agencia Española de Protección de Datos** (AEPD). Se rige también por el Título VI de la LOPD.

Las nuevas tecnologías han traído consigo el nacimiento de varias leyes que pretender regular el uso de aquellas. El 11 de julio de 2002 se desarrolló la Ley 34/2002 de **Servicios de la Sociedad de la Información** y de **Comercio Electrónico** (LSSICE). Esta ley regula, entre otras cosas, la celebración de contratos por vía electrónica, establece una serie de obligaciones y responsabilidades para los prestadores de servicios de la sociedad de la información (y de los intermediarios) y protege los intereses de los destinatarios de los servicios.

La Ley 59/2003, de 19 de diciembre, de **firma electrónica** nace para evitar que se frene el desarrollo de la sociedad de la información por la falta de confianza en la realización de transacciones telemáticas. La firma electrónica permite comprobar el origen y la integridad de los mensajes intercambiados a través de las redes de telecomunicaciones, brindando las bases para evitar el repudio, adoptando las medidas pertinentes basándose en fechas electrónicas.

Finalmente, sin querer adentrarme demasiado en materia legislativa, es de relevancia señalar que en la Constitución Española de diciembre de 1978 ya se alude a la regulación de la informática para proteger los derechos de las personas en el artículo 18 apartado 4 "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*".

1. 3 Características de la información

La información debe poseer una serie de características que hagan de ésta, una información de calidad. Carmen Pablos y otros autores recogen en su libro "*Informática y comunicaciones en la empresa*" las propiedades de la información que a continuación, son detalladas:

- Precisión: la información debe ofrecer exactamente lo que se pide de ella.
- Adecuación: se adapta a lo que se exige de ella.
- Fiabilidad: la información es veraz.
- Relevancia: responde a las necesidades del usuario.
- Exhaustividad: cualidad referente a la disposición de una amplia información relevante relacionada con el tema deseado.
- Puntualidad: la información es útil en el momento adecuado.
- Direccionamiento: debe dirigirse y recibirse por el individuo adecuado.
- Formato: la presentación de la información responde a las necesidades de la persona.
- Comprensibilidad: debe ser entendida por el usuario al que se dirige.
- Nivel de detalle: la información no es ni escasa ni desmesurada. Debe mostrar el nivel de detalle idóneo para el usuario que la tiene que manejar.
- Comunicabilidad: se divulga a través del medio apropiado.

1. 4 Sistemas de Información

Para recoger, procesar, almacenar y distribuir la información necesaria para que los trabajadores de la empresa puedan desempeñar su actividad de forma adecuada, se utilizan los Sistemas de Información.

Los Sistemas de Información (SI) son conjuntos organizados de elementos que procesan y distribuyen información con el fin de cumplir unos objetivos. No es necesario que estén basados en ordenadores. La utilización de aplicaciones informáticas sobre soportes informáticos da lugar a los Sistemas de Información Automatizados (SIA).

Los Sistemas de Información pretenden proporcionar una información oportuna y exacta para el apoyo en la toma de decisiones de la compañía. Además, garantizan la confiabilidad, la integridad y disponibilidad de la información. El uso de Sistemas de Información automatiza procesos operativos y pretenden conseguir ventajas competitivas en el mercado.

Entre las características que debe tener un Sistema de Información cabe destacar:

- ✓ El tiempo de respuesta del sistema debe ser el mínimo posible.
- ✓ La información que ofrece está disponible cuando es requerida.
- ✓ La información proporcionada es exacta y completa.
- ✓ Suministra el nivel de detalle de la información conforme con el propósito para el que se necesita.
- ✓ El sistema tiene capacidad de adaptación, es decir, flexibilidad.
- ✓ Es fiable y seguro.
- ✓ La interfaz es lo mas amigable posible para el usuario.

1. 4. 1 Elementos que conforman un Sistema de Información

Es posible distinguir cuatro elementos en un SI:

- **Información**: Todo aquello que el Sistema de Información recoge, procesa, almacena y distribuye.
- **Personas o usuarios**: Cualquier sujeto que introduce, procesa o utiliza la información del sistema, es decir, cualquier persona que interactúa con el SI.
- **Equipo de soporte**: El *hardware* y *software* empleado, además del papel, bolígrafos y demás elementos que puedan conformar el equipo de soporte para la comunicación.
- **Técnicas de trabajo**: Los métodos utilizados para desempeñar el buen funcionamiento de la empresa.

Los cuatro componentes anteriores se coordinan de forma adecuada para alcanzar los objetivos de la organización.

1. 4. 2 Actividades básicas de un Sistema de Información

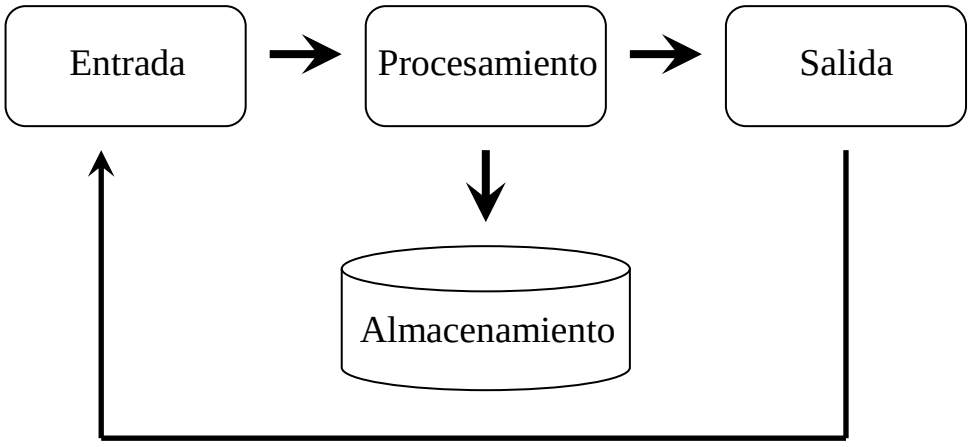
Existen cuatro actividades básicas que realiza un SI:

- **Entrada** de información: consiste en recoger los datos necesarios que se necesitan para procesar la información por medio de teclados, código de barras, etc. Pueden ser manuales (proporcionadas por el usuario) o automáticas (procedentes de un sistema).
- **Almacenamiento** de la información: proceso mediante el cual es posible recuperar la información guardada de procesos anteriores. Esta información suele almacenarse en ficheros.
- **Procesamiento** de información: los cálculos y operaciones realizadas sobre los datos. Transforma los datos recibidos en información útil para la toma de decisiones.

- **Salida** de información: es el resultado de la información obtenida en las actividades anteriores a través de impresoras y otros dispositivos. En ocasiones, la salida de información puede ser la entrada de ese u otro sistema.

En los Sistemas de Información puede existir **retroalimentación** (feedback) que consiste en que la información de la salida del sistema vuelve a él en forma de entrada. Es decir, la salida afecta al estado del sistema.

Figura 1.1 Actividades básicas de un Sistema de Información



1. 4. 3 Tipos de Sistemas de Información

Existen varios niveles en la planificación de las organizaciones y en cada nivel se utilizan diferentes sistemas de información. Se pueden destacar los siguientes:

- **Nivel operativo**: se utilizan **sistemas transaccionales**, también denominados OLTP (*On-Line Transactional Processing*) o TPS (*Transactional Processing System*). Estos sistemas se ocupan de recolectar información y de procesar transacciones como cobros o pagos.

  Los sistemas de procesamiento de transacciones automatizan actividades diarias de la compañía referentes a ventas y marketing, producción, finanzas, contabilidad y recursos humanos. Logran beneficios evidentes a corto plazo. El perfil de usuario que interactúa con el sistema es el personal de operaciones. Suponen un ahorro en la mano de obra y suele ser el tipo de sistema que primero se implanta.

- **Nivel táctico**: En este nivel se utilizan sistemas de información para la gestión y sistemas de apoyo a la toma de decisiones.

  - **Sistemas de información para la gestión**, también llamado sistemas de información gerencial o MIS (*Management Information System*). Suministra información para satisfacer gran parte de las necesidades de la gerencia. Estos sistemas aportan información de mayor calidad que el nivel anterior y generan informes resumidos que ayudan a la gerencia media a saber qué información necesitan recabar para tomar decisiones estructuradas.

  - **Sistemas de apoyo a la toma de decisiones** o DSS (*Decision Support System*). Se basa en el procesamiento y distribución de documentos para mejorar el rendimiento de la empresa. Proporciona información para apoyar la toma de decisiones.

    El perfil de usuario de DSS es la gerencia media-alta. Las decisiones que se toman son semiestructuradas o no estructuradas, es decir, no se goza de una respuesta precisa y clara.

- **Nivel estratégico**: Se utilizan **sistemas de soporte a la dirección** o ESS (*Executive Support System*) Está asociado a la alta dirección y pretende lograr ventajas competitivas en el mercado. Se deciden las líneas que deberá seguir la organización en el futuro, es decir, se trata de decisiones a largo plazo. Los informes que ofrecen estos sistemas son poco detallados y utilizan gráficos para facilitar la comprensión y comunicación a los directivos.

En las empresas, generalmente primero se implantan los sistemas transaccionales, posteriormente, se instauran los sistemas de información gerencial y sistemas de apoyo a las decisiones y finalmente, los sistemas estratégicos.

Figura 1.2 Niveles en la planificación de una compañía

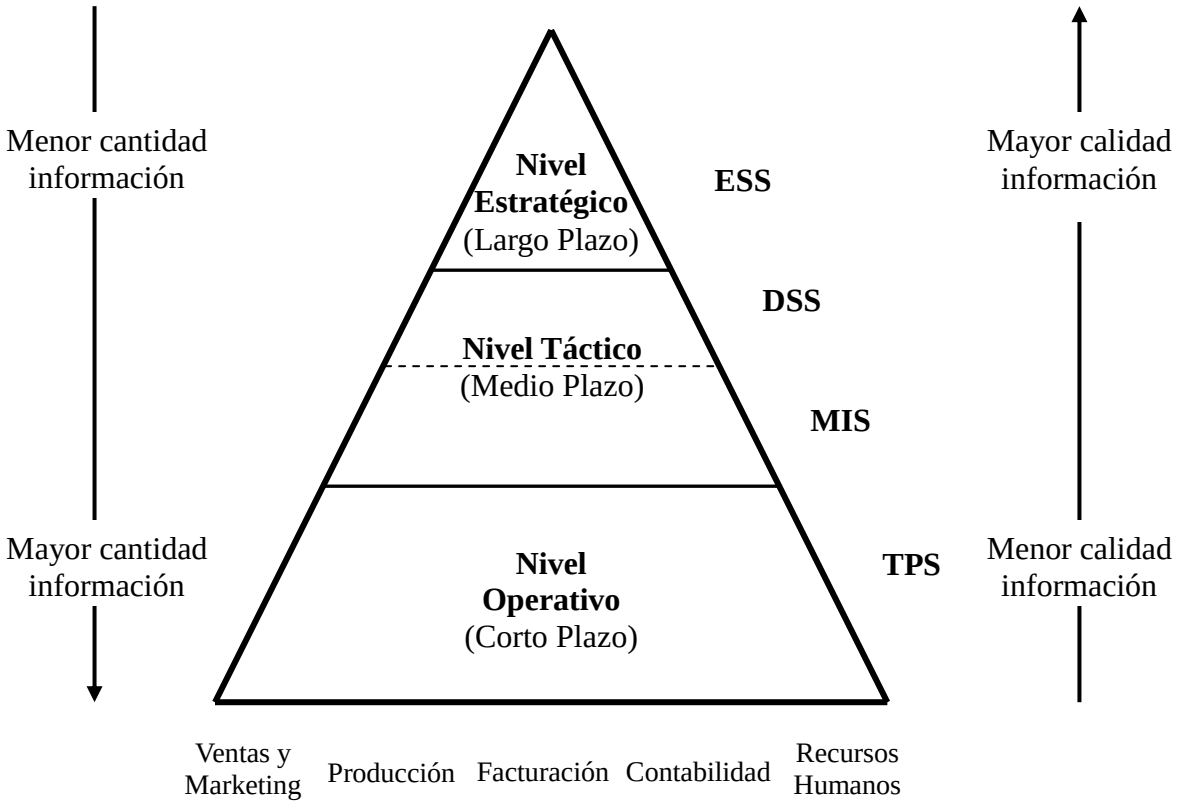


Figura 1.3 Sistemas de Información

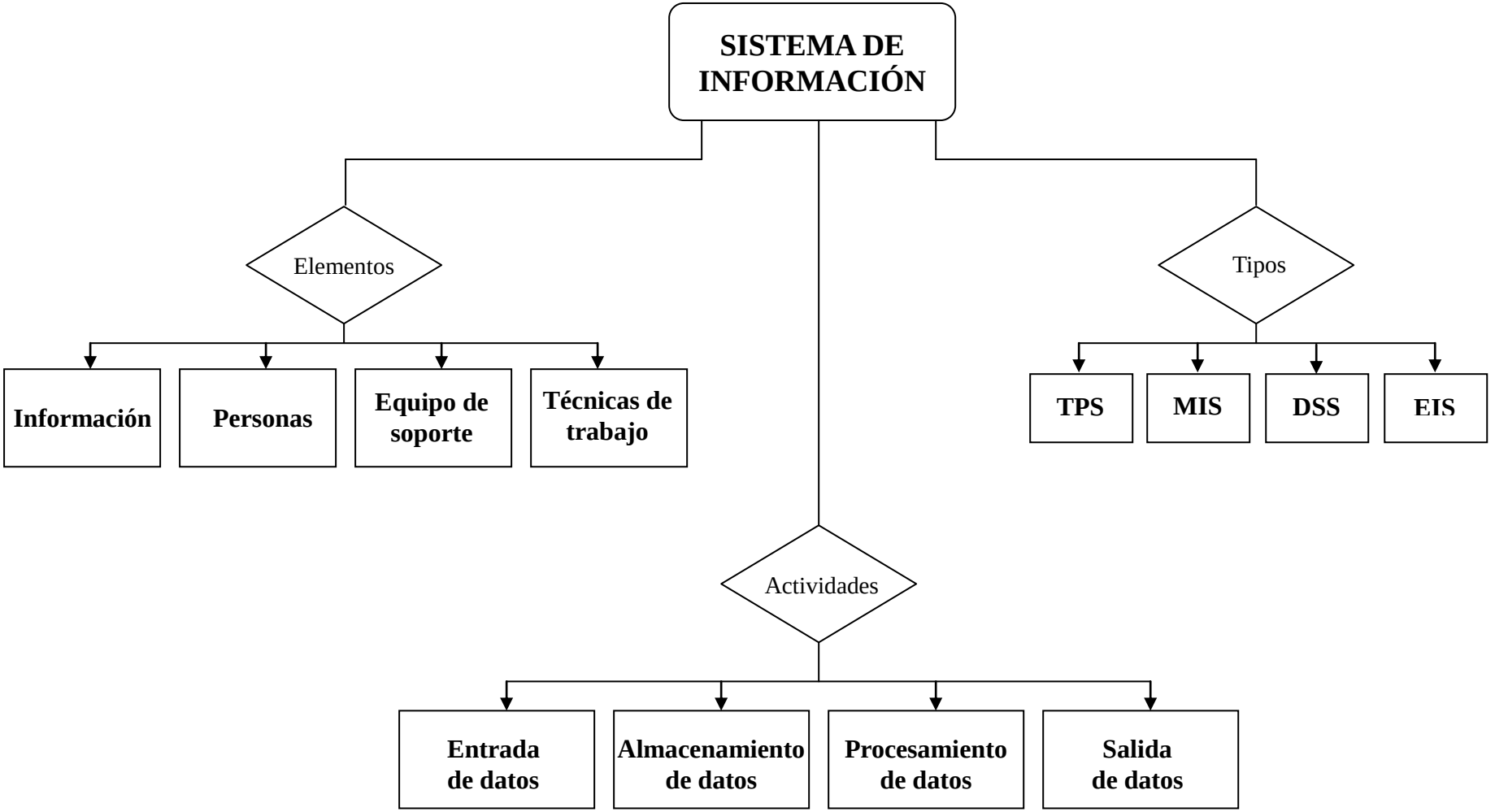
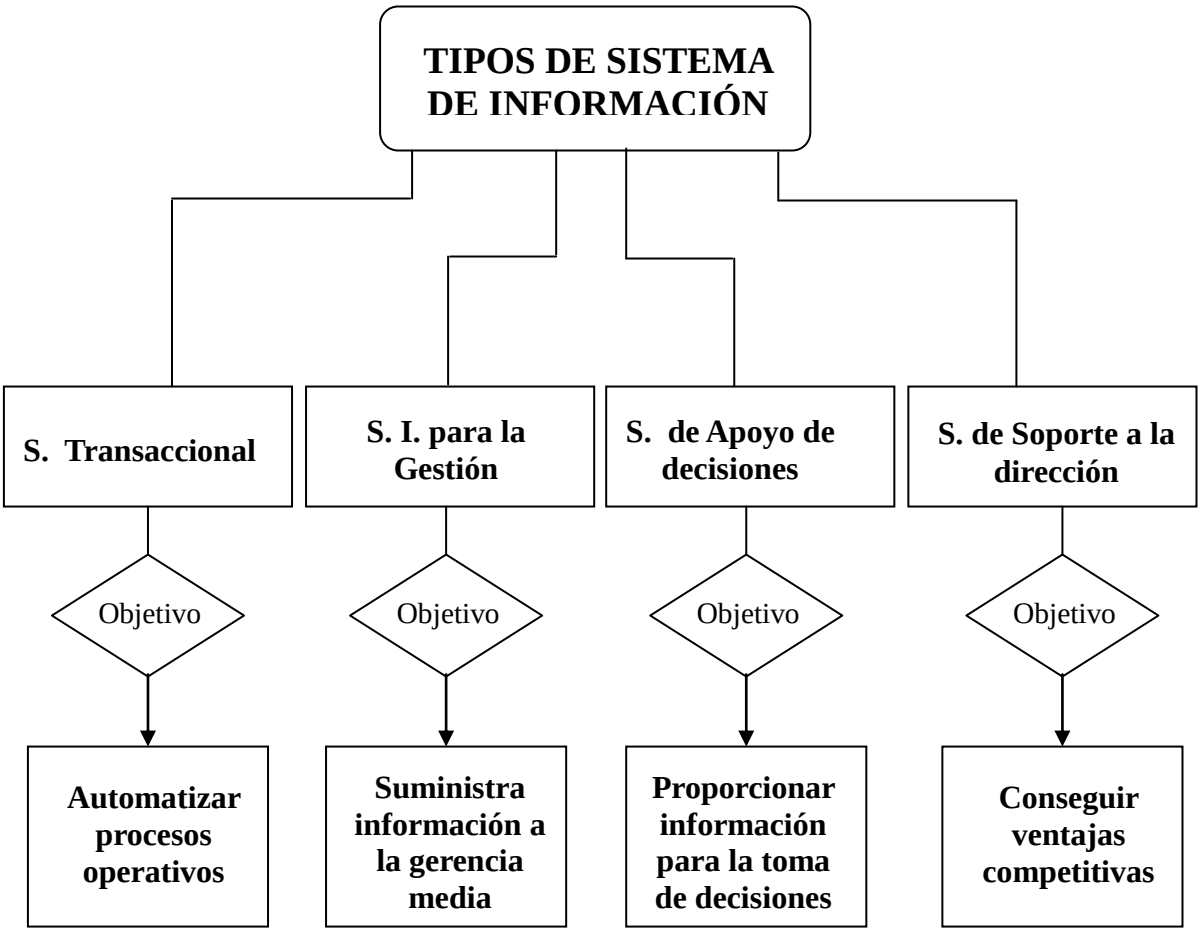


Figura 1.4 Tipos de Sistemas de Información



II. SEGURIDAD

2. 1 Introducción

La seguridad se puede definir como aquello que *esta "libre de peligro, daño o riesgo*". Pero lo cierto es que la seguridad plena no existe, por lo que otro enunciado que podría encajar mejor con la realidad sería "*calidad relativa, resultado del equilibrio entre el riesgo (amenazas, vulnerabilidades e impacto) y las medidas adoptadas para paliarlo*".

Una definición que se ajusta más en el ámbito informático es: "*la seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles*". Esta definición está incluida en el libro I - Método de MAGERIT versión 2.

La seguridad no es un lujo que se puedan permitir algunas empresas, sino que es una necesidad de supervivencia. Desafortunadamente, hoy en día muchas organizaciones no invierten suficientes recursos en seguridad.

La falta de seguridad puede deberse a dos factores:

- Desconocimiento de las posibles amenazas que pueden desencadenar un incidente en la entidad.
- Falta de conocimiento de las medidas de seguridad que existen para paliar las amenazas que pueden producir daños materiales o inmateriales en los activos.

Evidentemente, a mayor seguridad, mayor coste. Por este motivo, se debe lograr un equilibrio entre ambos teniendo siempre en cuenta las limitaciones de la organización. Es bien conocido por todos el dicho de que "*es mejor prevenir que curar*" y el coste de la no seguridad puede llegar a causar una cuantía desmesurada.

En ocasiones, el coste de asegurar algunas posesiones de la empresa puede resultar más costoso que producirlas de nuevo. Por lo tanto, el coste de las salvaguardas nunca debe sobrepasar el coste del activo protegido. Además, dependerá de la entidad el nivel de seguridad que se deba aplicar y en qué posibles amenazas y vulnerabilidades proporcionar especial atención. Es prácticamente imposible conseguir una seguridad total en la compañía porque el coste sería excesivo.

Es complicado concienciar al personal de la empresa de la importancia de la seguridad sin que se distraigan de su actividad diaria o sin que se incida en grandes costes. Es fácil encontrar empleados que desconocen el número de incidentes de seguridad que sucedieron el año anterior en su empresa o el origen de éstos (fallos de empleados, troyanos, virus...). Es primordial que la entidad informe y conciencie a todas las áreas de los riesgos a los que se enfrentan.

Las organizaciones evolucionan con el paso del tiempo. De la misma forma que van surgiendo nuevas amenazas que ponen en riesgo los recursos de la compañía que pueden hacer peligrar la continuidad del negocio. Debemos intentar transformar los riesgos en fortalezas.

2. 2 Bienes a proteger

Debemos tener muy claro qué activos de nuestra empresa queremos proteger, de qué queremos salvaguardarlos y cómo queremos hacerlo.

Los elementos que han de ser protegidos son:

- **Datos**: Es lo más valioso a proteger. Es la información lógica de la organización, resultado de la labor realizada.
- ***Software*** (Sw.): Es el conjunto de programas, instrucciones y reglas informáticas que hacen funcionar el *hardware*.
- ***Hardware*** (Hw.): Es el conjunto de componentes que integran la parte física de una computadora.
- **Elementos fungibles**: Son aquellos que se gastan o se desgastan con el uso continuo, como el tóner, los cartuchos o los DVDs.

Se debe contar con un inventario de todos los activos importantes de la compañía que incluya toda la información necesaria acerca del activo como: el tipo de activo, lugar de ubicación, valor comercial y todo dato relevante para la empresa. Además, cada activo debe tener un propietario que se haga responsable de su mantenimiento.

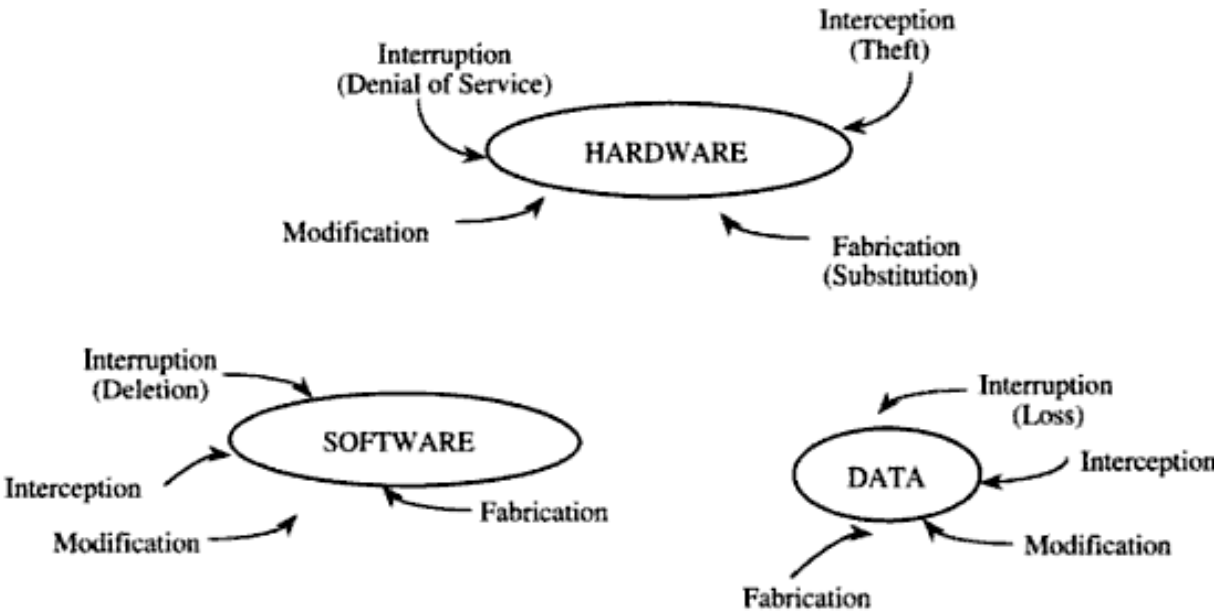
2. 2. 1 Tipos de ataques a los bienes de la empresa

Los ataques que puede sufrir una empresa pueden ser de diferente índole:

- **Alteración o Manipulación**: Se obtiene el activo y se manipula ya sea para modificarlo o destruirlo. Es un ataque que afecta a la integridad de los datos.
- **Intercepción o Monitorización**: Apoderarse de un bien de la empresa o acceder al contenido del mismo sin autorización. Vulnera la confidencialidad de la información.
- **Fabricación o Suplantación**: Elaborar recursos similares a los interceptados, quebrantando la autenticidad de los datos.
- **Interrupción o Denegación de servicio**: El activo resulta inutilizable o no disponible, afectando así, a la disponibilidad de la información.

A continuación, se muestra una figura muy sencilla que expone de manera gráfica los ataques que pueden sufrir los recursos de la empresa.

Figura 2.1 Ataques a los recursos de la empresa



Fuente: "*Security in computing*". Shari Lawrence Pfleeger y Charles P. Pfleeger. Editorial Prentice Hall.

2. 2. 2 Agentes que pueden causar daños en la organización

En general, es posible distinguir tres grandes grupos que pueden dañar los activos de la compañía:

- **Personas**: Personal de la empresa, antiguos empleados, piratas, terroristas, curiosos o intrusos remunerados.
- **Catástrofes**: Pueden ser desastres naturales o del entorno.
- **Amenazas lógicas**: Virus, gusanos, caballos de Troya, puertas traseras o bombas lógicas, entre otras. Este apartado se ampliará en el capítulo de Seguridad Lógica.

2. 2. 2. 1 Personas causantes de incidencias

Los responsables de incidentes pueden ser trabajadores de la compañía o personas externas. Implantar las medidas oportunas para evadir o disminuir incidentes es vital para evitar sorpresas desagradables.

Según la actitud del atacante se distinguen dos grupos:

- **Atacantes activos**: Estos ataques interfieren en el buen funcionamiento del sistema cambiado el estado de la información.
- **Atacantes pasivos**: Fisgonean en el sistema pero no lo modifican aunque sí atentan contra la confidencialidad. Son difíciles de detectar ya que no provocan ninguna alteración en los datos.

2. 2. 2. 1. 1 Empleados

Aproximadamente, entre el 60% y el 80% de los daños producidos en la organización son causados por personal interno de la empresa. Los trabajadores de la compañía pueden causar incidentes de forma voluntaria o inconsciente:

- **Amenazas accidentales**: Se producen incidentes de manera involuntaria, generalmente por falta de cultura de seguridad. Pueden producirse por desconocimiento de las normas básicas de seguridad o porque ni siquiera estén implantadas en la organización.

  Ejemplos de malas prácticas por parte de trabajadores de la empresa que pueden causar daños de forma involuntaria a la compañía son:

  - Empleados que en la hora de la comida no bloquean o apagan el ordenador.
  - Contraseñas escritas en pósit a la vista de todos.
  - Visitar el correo electrónico personal desde el ordenador de la empresa.
  - Transferir archivos de la compañía al ordenador personal del trabajador.
  - Mantener conversaciones confidenciales en lugares públicos o en oficinas de la empresa no habilitadas para ese propósito.

Para acabar con estas malas prácticas se debe concienciar a toda la plantilla de la importancia de la seguridad y de los daños que pueden causar la no preocupación por la seguridad de la organización.

- **Amenazas intencionadas**: A veces, los trabajadores pueden cometer actos maliciosos de forma voluntaria para perjudicar a la compañía. Un ataque realizado por un empleado suele ser más difícil de detectar y más efectivo que el que pueda realizar una persona ajena a la entidad. Esto es debido a que el empleado conoce la compañía desde dentro, sus puntos fuertes y débiles.

  Las infracciones intencionadas más habituales por parte de empleados son:

  - Daños informáticos

    Se producen eliminando, modificando o inutilizando datos o programas de la organización. Suelen originarse por un despido que el empleado no asume o por un enfrentamiento entre la compañía y el trabajador. Lo más habitual es introducir virus en los ordenadores de la empresa, el sabotaje y las bombas lógicas.

  - Uso excesivo de recursos informáticos

    Especialmente el acceso a Internet no relacionado con el propósito de la organización, o bien, por la extralimitación en su uso.

  - Acceso a información confidencial y datos personales

    Se difunde información confidencial o se revela datos personales de empleados o clientes a terceros (clientes, competidores...). La divulgación no autorizada de datos se denomina también ***data leakage***.

    No requiere un uso de técnicas demasiado elaboradas para obtener tales datos, basta con disponer de un dispositivo de almacenamiento en el que copiar la información importante para obtener algún tipo de beneficio.

Un empleado podría copiar información relevante de un ordenador referente a un proyecto que estuviese realizando la organización, con el fin de facilitársela a la competencia y lograr con ello un beneficio económico. La entidad competidora utilizaría esa información para perjudicar económicamente a la empresa, plagiando el proyecto o sacándolo antes al mercado, logrando así, una ventaja competitiva.

Frecuentemente, se utilizan esos datos para chantajear a la empresa o para venderlos a un tercero. Esta práctica se evita en parte, implantando controles de acceso a la información confidencial.

- Crear empresa competidora utilizando activos inmateriales de la compañía

El empleado se adueña de información de la empresa en la que trabaja utilizando soportes informáticos o Internet en beneficio de su nueva empresa.

- Amenazas, injurias y calumnias

Las amenazas buscan algún tipo de beneficio para el propio empleado. Las injurias y las calumnias buscan dañar la imagen de la compañía o desacreditarla. Generalmente se realizan a través de cuentas de correo que pueden ser de la empresa o anónimas.

- Copiar activos inmateriales de la compañía

Se duplican activos inmateriales de la organización, sobre todo, obras protegidas por la propiedad intelectual para entregárselas a terceros.

- Intercambio de obras de terceros a través de redes P2P

El empleado descarga o sube a la red archivos de terceros y convierte a la compañía en proveedora de copias ilegales de música, películas o de programas.

2. 2. 2. 1. 1. 1 Pautas para evitar daños causados por empleados

Existen pautas para disminuir el daño que pudiera causar un trabajador en la entidad. Algunas medidas a poner en práctica son las siguientes:

⇒ **Investigar y verificar el currículum** de los trabajadores: no basta con leer por encima un curriculum de un aspirante a empleado, sino que también hay que verificarlo. Es posible que ese individuo haya sido despedido de alguna de las empresas por realizar acciones maliciosas contra la compañía a la que pertenecía.

Por tanto, los antecedentes de los trabajadores han de ser convenientemente investigados, en especial, aquellos cuyas funciones estén relacionadas con el acceso a información confidencial.

⇒ **Rotación de funciones**: se realizan para evitar rutinas y, sobre todo, por seguridad. El conocimiento parcial puede derivar en una complicidad entre los trabajadores. Para evitarlo, lo más efectivo es rotar asumiendo diferentes responsabilidades dentro de la empresa lo que permite a los empleados establecer una vigilancia recíproca.

⇒ **Inhabilitar cuentas** cuando finalice la actividad en la empresa: es importante que en el momento en el que un trabajador deje de serlo, suspender el acceso a sus cuenta o cambiar las contraseñas y controlar su acceso a las instalaciones utilizando las mismas medidas de seguridad que si se tratase de cualquier persona externa.

Además, deben devolver todos los activos que posean de la compañía al finalizar su actividad. El exceso de confianza que la empresa pueda mostrar hacia un antiguo empleado, puede tener consecuencias fatales para la compañía.

⇒ **Necesidad de conocimiento** o *Need to know*: los trabajadores deben disfrutar del mínimo privilegio que necesiten para realizar su actividad dentro de la empresa.

⇒ **Conocimiento parcial** o *Dual control*: existen tareas en la empresa que han de ser realizadas por dos empleados, ya que si sólo existe una persona con conocimientos sobre esa actividad, al despedirse de la empresa o al marcharse de vacaciones, no se podrá seguir realizando esa tarea hasta que el trabajador se incorpore a su puesto o sea remplazado.

Además, esta práctica es necesaria porque si se comete un fallo o un acto malicioso, de esta forma existirá otra persona que pueda solventar el daño.

⇒ **Separación de funciones**: se debe delimitar y separar las funciones de cada empleado para evitar posibles incidentes.

2. 2. 2. 1. 2 Terceros

Personas externas a la empresa cometen robos o fraudes con ánimo de lucro. Buscan apropiarse de activos de la organización o incumplir leyes en busca de un beneficio personal o de un tercero sin que exista la participación de un empleado de la entidad.

En este apartado se engloban los siguientes grupos:

- **Ex-empleados**: son personas que han sido despedidas y no están conformes con esa decisión o bien han decidido trabajar para la competencia.
- **Terroristas**: atacan el sistema para causar algún daño sobre el mismo. Suele realizar ataques de modificación o de borrado de datos.
- **Curiosos**: tienen gran interés en las nuevas tecnologías, pero no disponen de los conocimientos ni experiencia suficiente para considerarlos *hackers* o *crackers*. No suelen causar daños importantes.
- ***Crackers***: Personas con amplios conocimientos informáticos cuyo objetivo es acceder a un sistema informático ilegalmente para realizar alguna acción maliciosa.

  Existen varios tipos de *crackers* según las acciones que realizan:

  - *Carding* o Tarjeteo: uso ilegal de tarjetas de crédito de otras personas.
  - *Trashing* o Basureo: rastrean papeleras en busca de información como contraseñas, directorios o números de tarjetas de crédito.

- *Phreaking* y *Foning*: utilización de redes telefónicas de manera ilegal.
- Piratas: copian de forma ilegal música, películas o *software* legal con fines lucrativos.

- **Intrusos remunerados**: son muy peligrosos aunque no suelen ser muy habituales. Tienen mucha experiencia y los conocimientos suficientes para robar información o dañar de alguna forma a la empresa atacada, remunerados por otro agente externo.

Algunas prácticas deshonestas que realizan personas ajenas a la empresa son:

➢ Chantajes, sobornos y extorsión

La empresa es sometida a chantajes y extorsiones por parte de personal externo en busca de un beneficio. La entidad también puede recibir un soborno o incentivo por parte de un proveedor o de una compañía asociada.

➢ Robo de activos de la empresa

Se consiguen activos, generalmente inmateriales, de la empresa para uso propio o para cederlos a otros con fines maliciosos.

➢ Estafas y fraudes a la entidad

La compañía es sometida a un fraude o estafa.

➢ Robo de identidad de un empleado para cometer actos delictivos

Apropiación de claves o contraseñas de empleados para suplantar su identidad y acceder a información privada de la empresa.

Aproximadamente, sólo uno de cada cuatro incidentes provocados por empleados o personal externo a la empresa es llevado a los tribunales. Algunos de los motivos por los que las entidades no denuncian o no dan a conocer su situación son:

✓ Por mala imagen y publicidad.

✓ Por miedo a que la competencia se beneficie del incidente.

✓ Porque la compañía cree más conveniente resolverlo internamente.

✓ Por desconocimiento legal sobre este tipo de incidentes.

2. 2. 2. 2 Catástrofes

Es importante proteger los activos de posibles daños físicos que pudieran afectar a la entidad. De nada sirve poner toda la atención en la seguridad lógica si un incendio puede acabar con todos los bienes de la compañía.

Existen catástrofes cuya probabilidad de materializarse es mínima como, por ejemplo, un ataque nuclear o la caída de un misil. Cuando la probabilidad de ocurrencia es muy baja lo normal es aceptar el riesgo ya que implementar algunas medidas supondría un coste bastante alto para la baja probabilidad de materialización de dicho riesgo.

Las catástrofes se pueden dividir en dos grupos:

- **Desastres naturales**: La posibilidad de controlar la naturaleza es casi nula, aunque muchas catástrofes naturales son predecibles. Algunas se pueden evitar en mayor o menos medida. Por ejemplo, evitar construir una sede de la organización en zonas sensibles a sufrir terremotos, riadas o incendios.
    - **Inundaciones**: pueden ocurrir por causas naturales o provocadas por sofocar un incendio. Se podrían prevenir, instalando mecanismos de detección que apaguen los sistemas si se detecta agua y corten la corriente. Además, es necesaria la existencia de sistemas de evacuación de agua en el caso de que se produzca la inundación.
    - **Humedad**: en entornos normales, niveles aceptables de humedad son necesarios para evitar la electricidad estática pero demasiada humedad puede estropear los recursos de la empresa. Para controlar la humedad basta con instalar alarmas que nos informen de niveles anormales de humedad.
    - **Condiciones climatológicas**: como fuertes tormentas, tempestades... que pueden dañar los activos de la organización. Se ha de colocar pararrayos y demás artilugios necesarios en el caso que se produjese cualquier condición climatológica adversa.

- **Terremotos**: fenómenos sísmicos que según su intensidad pueden llegar a destruir edificios y cobrase vidas humanas. Para prevenirlos, se deben construir edificios asísmicos, fijar los equipos y alejar los objetos de las ventanas.
- **Incendios y humo**: El origen del fuego puede darse por varias causas como, por ejemplo, un cortocircuito en las instalaciones eléctricas o el uso inadecuado de materiales combustibles causando daños importantes en la organización. Se deben instalar detectores de incendios y de humo, extintores y realizar revisiones periódicas de éstos.

- **Desastres del entorno**:
  - **Señales de Radar**: Las señales de radar pueden afectar al procesamiento electrónico de la información si alcanza, al menos, los 5 voltios/metro.
  - **Instalaciones eléctricas**: Las subidas y caídas de tensión junto con el ruido interfieren en el funcionamiento de los componentes electrónicos. Existe la posibilidad de que se produzcan cortes de electricidad.

    Para los cortes de suministro eléctrico, se puede utilizar Sistemas de Alimentación Ininterrumpida (SAI) que son equipos que disponen de baterías permitiendo mantener varios minutos los aparatos conectados a ellos, consintiendo que los sistemas se apaguen de forma ordenada.

    Además, existe el riesgo de corte de cables, deterioro o interferencias. Lo más favorable sería acoplar los cables a la estructura del edificio, instalar tomas de tierra, colocar filtros si existe ruido eléctrico (o alejar el *hardware* si fuera posible), colocar generadores y estabilizadores de tensión.
  - **Temperaturas extremas**: Las temperaturas extremas ya sean exceso de frío o calor dañan gravemente los equipos. En general, el rango de temperatura debe oscilar entre los 10º C y los 32º C. Para ello, se debe instalar sistemas de calefacción y aire acondicionado, además de asegurarse la correcta ubicación y ventilación de los equipos.

Figura 2.2 Activos de la organización

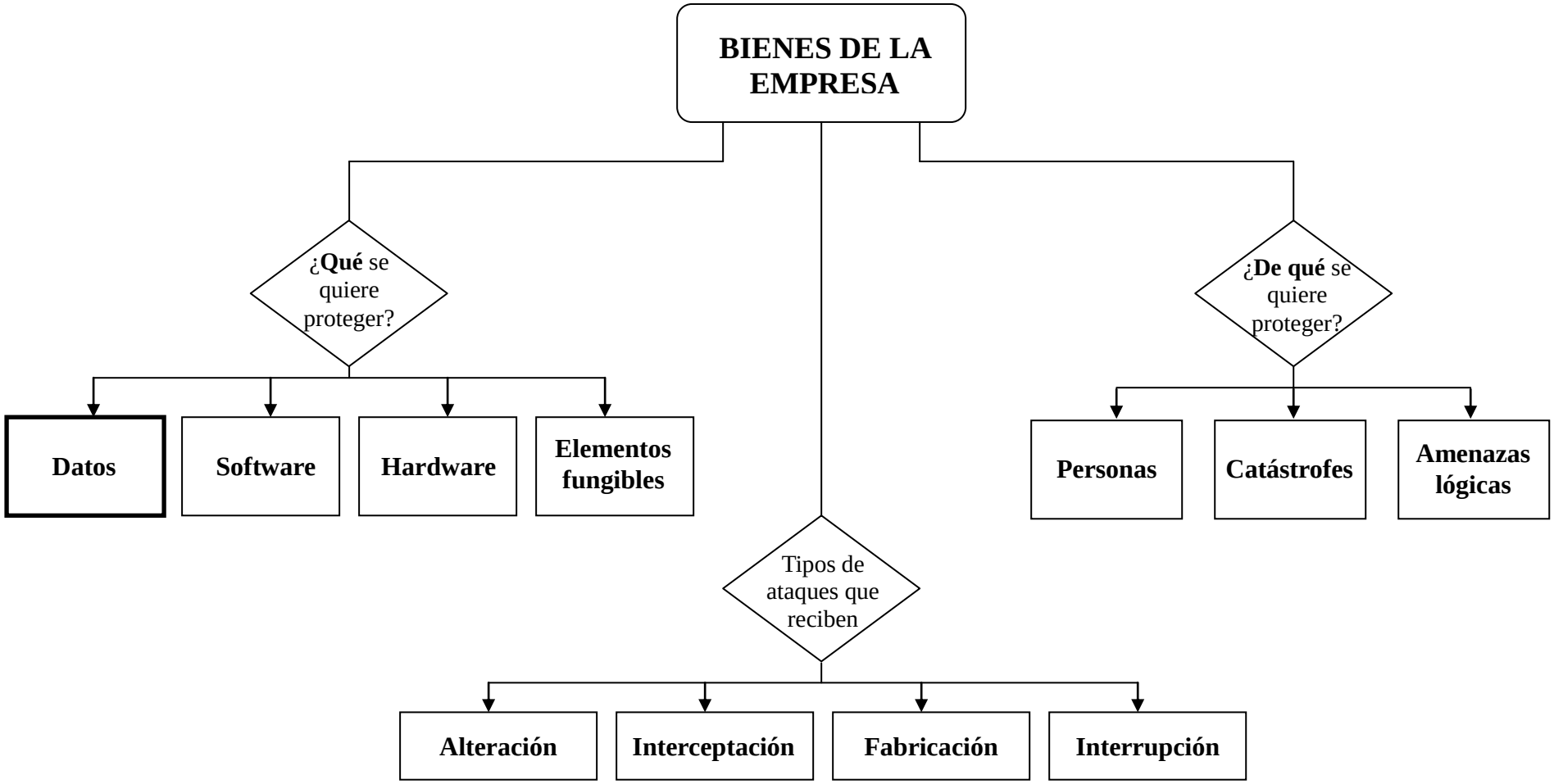


Figura 2.3 Personas causantes de incidentes

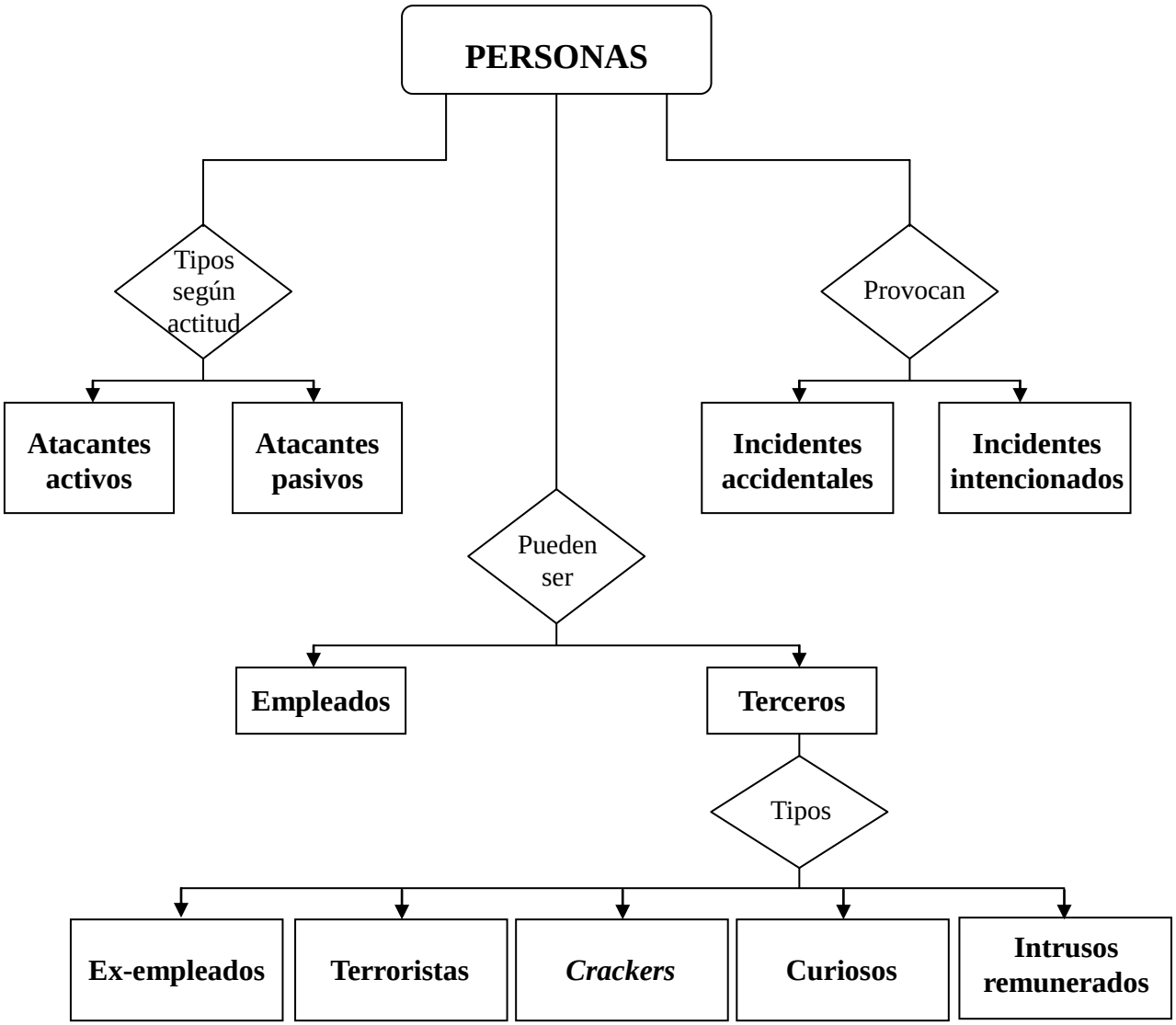
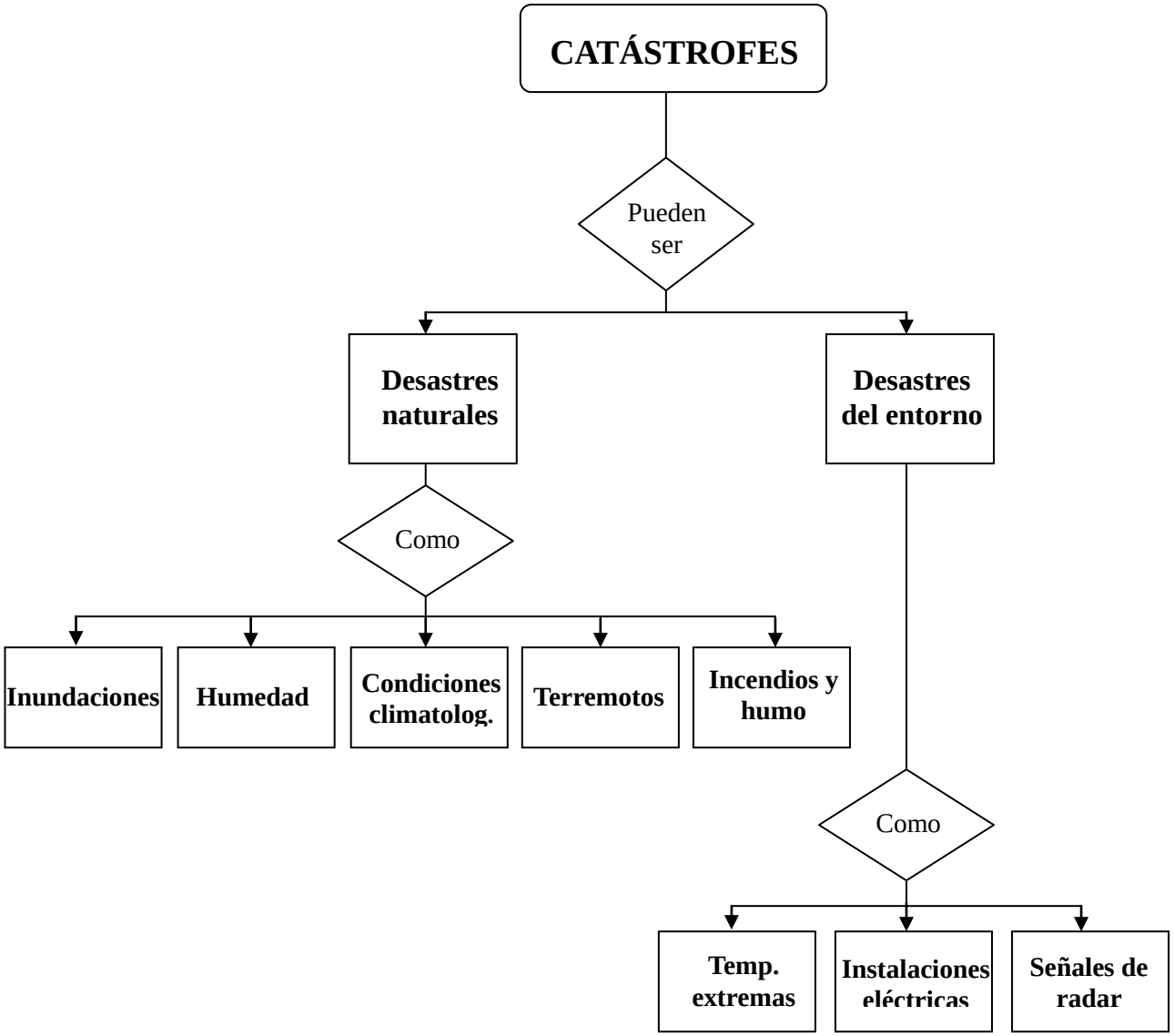


Figura 2.4 Catástrofes que puede sufrir una entidad

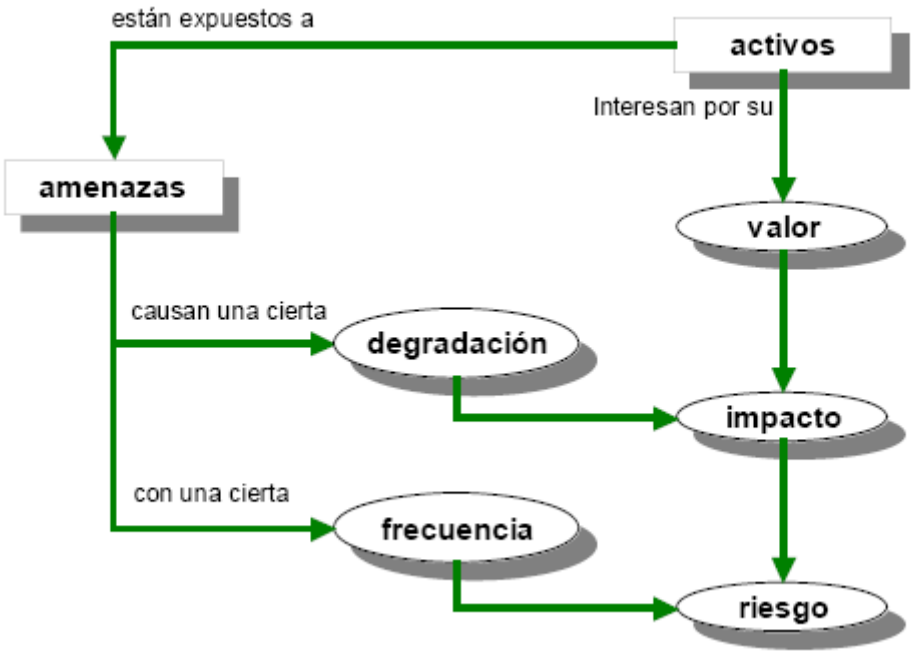


2. 3 Análisis de riesgos

Para definir lo que entendemos por riesgo, es esencial puntualizar una serie de términos fundamentales. En una organización es posible que se produzcan incidentes que dañen sus activos. El evento que puede desencadenar dicho incidente es lo que se denomina **amenaza**. La posibilidad de que se materialice la amenaza sobre un activo es una **vulnerabilidad**. Las vulnerabilidades se miden por la probabilidad de ocurrencia de la amenaza y la frecuencia con la que se produce.

Si la amenaza se materializara, es necesario estimar cuanto degradaría el activo afectado. La consecuencia que dicha materialización tiene sobre el activo es un **impacto**. El impacto puede ser de tipo cuantitativo (pérdidas económicas) o cualitativo (imagen de la empresa, responsabilidad legal, etc.) La posibilidad de que se produzca un impacto en la organización es lo que se conoce como **riesgo**.

Figura 2.5 Conceptos básicos en el análisis de riesgos



Fuente: MAGERIT versión 2, libro I "*Método*" (2006). Ministerio de Administraciones Públicas.

Nuestra empresa está expuesta a posibles amenazas que pueden materializarse en cualquier momento. Por esta razón, se debe evitar o minimizar las consecuencias no deseadas en los bienes de la entidad.

Por ejemplo, una empresa podría sufrir un incendio o no sufrirlo, pero debe implantar medidas para que no ocurra y si sucede, saber de antemano qué secuelas dejaría en la compañía e intentar minimizarlas lo máximo posible.

Las amenazas siempre han existido pero con la llegada de los ordenadores han aumentado considerablemente. Cada vez son más frecuentes, más difíciles de detectar y más perjudiciales para las empresas.

En ocasiones, la realidad supera la ficción y cuando vemos películas en las que el protagonista consigue acceder a datos confidenciales de clientes de un banco y consigue extraer millones de dólares de sus cuentas, no imaginamos que pueda suceder en la realidad. En cambio, existen casos en la vida real que reflejan que esto puede ocurrir, por lo que identificar todos los riesgos a los que se expone la organización es vital para saber a que nos enfrentamos.

Es recomendable realizar un análisis de riesgos para eliminar riesgos o atenuarlos en el caso de no poder eliminarlos. Un análisis de riesgos estudia, mide, evalúa y previene los riesgos que pueden desencadenar incidentes que afecten a la compañía.

Se pretende identificar los contratiempos que podrían materializarse, analizar las circunstancias que tendrían que presentarse para que el incidente se produjese y valorar las consecuencias que esto tendría.

Es evidente, por tanto, que analizar los posibles riesgos a los que se expone la compañía es una actividad de alta prioridad. Además, el análisis de riesgos se puede realizar antes o después de la definición de una política de seguridad.

2. 3. 1 Etapas del análisis de riesgos

Juan Gaspar diferencia las siguientes etapas de un análisis de riesgos, en su libro "*Planes de Contingencia: la continuidad del negocio en las organizaciones*":

i.**Analizar y reducir los riesgos** a los que se expone la organización:

Lo primero es identificar los posibles daños o peligros a los que se expone la compañía ya que si no se conocen difícilmente se sabrá que medidas se deben tomar. Algunos métodos para identificar riesgos son:

- ✓ Tormenta de ideas (*Brainstorming*)
- ✓ Historial de incidentes ocurridos propios y ajenos
- ✓ Juicios basados en la experiencia
- ✓ Diagramas de flujo
- ✓ Organigramas
- ✓ Encuestas y cuestionarios
- ✓ Análisis de sistemas
- ✓ Análisis de escenarios
- ✓ Entrevistas
- ✓ Consultas con expertos

Además, en cualquier riesgo se ha de tener en cuenta:

- El **valor** de los activos: no es lo mismo el valor que pueda tener la información generada durante el último trimestre que el valor de una impresora que deje de funcionar.
- La **frecuencia** de la amenaza: el número de veces que se repite en un periodo de tiempo.
- El **impacto**: las consecuencias del daño que causa en la empresa.
- La **incertidumbre**: es el grado de desconocimiento que tenemos de que la amenaza se materialice en un futuro.
- La **eficacia** de las medidas de seguridad: la comprobación de que realmente aplicando esos mecanismos de seguridad se consigue paliar el riesgo.

- El **coste** de las medidas de seguridad adoptadas: el coste de las medidas debe ser proporcional al valor de los activos que se están protegiendo. Incluye el coste de implantarlas, mantenerlas, reponerlas y adaptarlas.

Una vez conocidos los riesgos se buscan los mecanismos a aplicar. El análisis de riesgos lo puede realizar personal externo o interno pero en cualquiera de los dos casos es imprescindible el uso de metodologías como:

a) **MAGERIT** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las administraciones públicas): estudia los riesgos que soporta un Sistema de Información y su entorno, además de recomendar las medidas que deberían adoptase.

b) **MARION**: evalúa el nivel de seguridad utilizando cuestionarios ponderados. Las respuestas son cualitativas.

c) **MEHARI**: clasifica los riesgos según las causas y las característica de seguridad que vulnera (confidencialidad, integridad y disponibilidad).

d) **Modelo de McCumber**: es independiente del entorno, arquitectura o tecnología que gestiona la información. Para asegurar la confidencialidad, integridad y disponibilidad de la información clasifica las medidas de seguridad en tres grupos:

   d.1) **Medidas tecnológicas**: dispositivos físicos o lógicos que aseguran las características de la información.

   d.2) **Normas y procedimientos**: solucionan carencias en la seguridad de la información.

   d.3) **Formación y entrenamiento**: el personal de la organización debe mentalizarse de la importancia de la seguridad.

   Cada vulnerabilidad encontrada conlleva una medida de seguridad a llevar a cabo.

ii. **Identificación de amenazas y vulnerabilidades**:

Se definen las amenazas a las que la organización está expuesta. Una buena opción es utilizar la metodología de MAGERIT que agrupa las amenazas (de accidentes, de errores, amenazas intencionales presenciales...).

iii.**Identificación de riesgos potenciales,** la probabilidad y las consecuencias:

Cuanto más detallado sea el análisis mejor. Se debe establecer prioridades en la implantación de las medidas. Es posible utilizar la metodología MARION que agrupa las preguntas de los cuestionarios en 27 factores donde cada pregunta está ponderada según su impacto en la seguridad del sistema. Existen factores de prevención y de protección.

iv. **Posibles alternativas frente al riesgo**

La dirección de la organización debe considerar alternativas ante los riesgos que se detecten:

- **Evitar** el riesgo: Es una solución de carácter preventivo. Por ejemplo, si el lugar donde se quiere construir una nueva sede de la organización es una zona expuesta a tormentas, ventiscas o inundaciones, habría que plantearse la idea de buscar otro lugar para su localización menos expuesto a desastres naturales.
- **Minimizar** el riesgo: Cuando no es posible eliminar un riesgo se debe reducir al máximo la probabilidad de que se materialice y/o el impacto que pueda causar en la organización.

  Por ejemplo, no se puede evitar un incendio, pero si es posible minimizar sus causas impidiendo que se fume en las instalaciones, además de contar con las medidas oportunas que tendrían que llevarse a cabo si se produce el fuego como la presencia de detectores de incendios, extintores… y contando con copias de seguridad en otros edificios.
- **Asumir** el riesgo: Es posible que el coste de eliminar el riesgo sea demasiado alto o que la probabilidad de ocurrencia sea muy baja y la compañía deba aceptar esos riesgos.

- **Transferir** un riesgo: Cuando no es posible eliminar o reducir el riesgo, una alternativa es transferirlo, por ejemplo, por medio de pólizas de seguro.
- **Eliminar** el riesgo: Es bastante improbable que se pueda eliminar un riesgo totalmente pero sí disminuirlo, suprimiendo la mayoría de sus causas.

2. 3. 2 Decidir quién debe realizar el análisis de riesgos

Para la elaboración del análisis es posible utilizar recursos externo o de la propia compañía:

- **Personal externo**: La ventaja de contratar consultores externos es que no tienen relación directa con la organización y, por tanto, serán totalmente objetivos. Además, es posible que para la compañía sea más rentable que su personal dedique su tiempo a otras actividades.
- **Personal interno**: Conocen la organización desde dentro, pero no deben perder nunca la objetividad. Han de tener la formación y experiencia necesaria para llevar a cabo el análisis de riesgos.

Figura 2.6 Análisis de riesgos

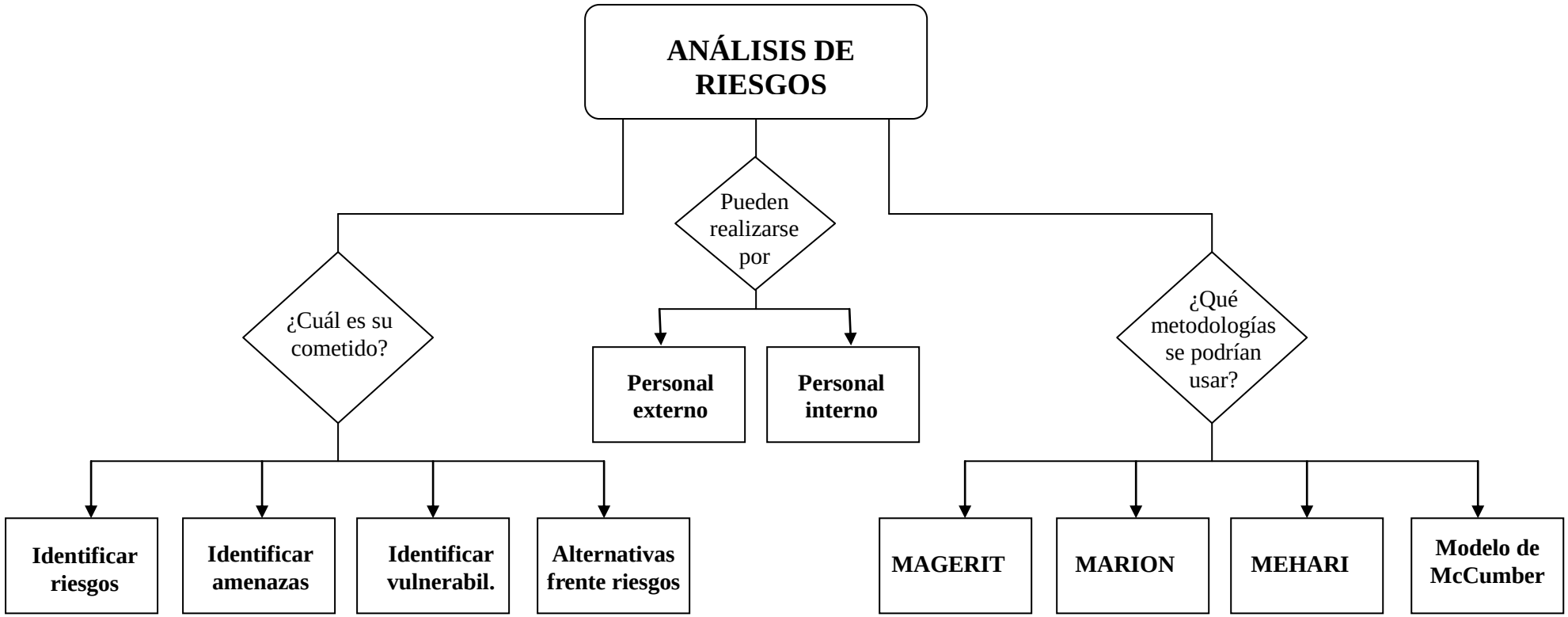
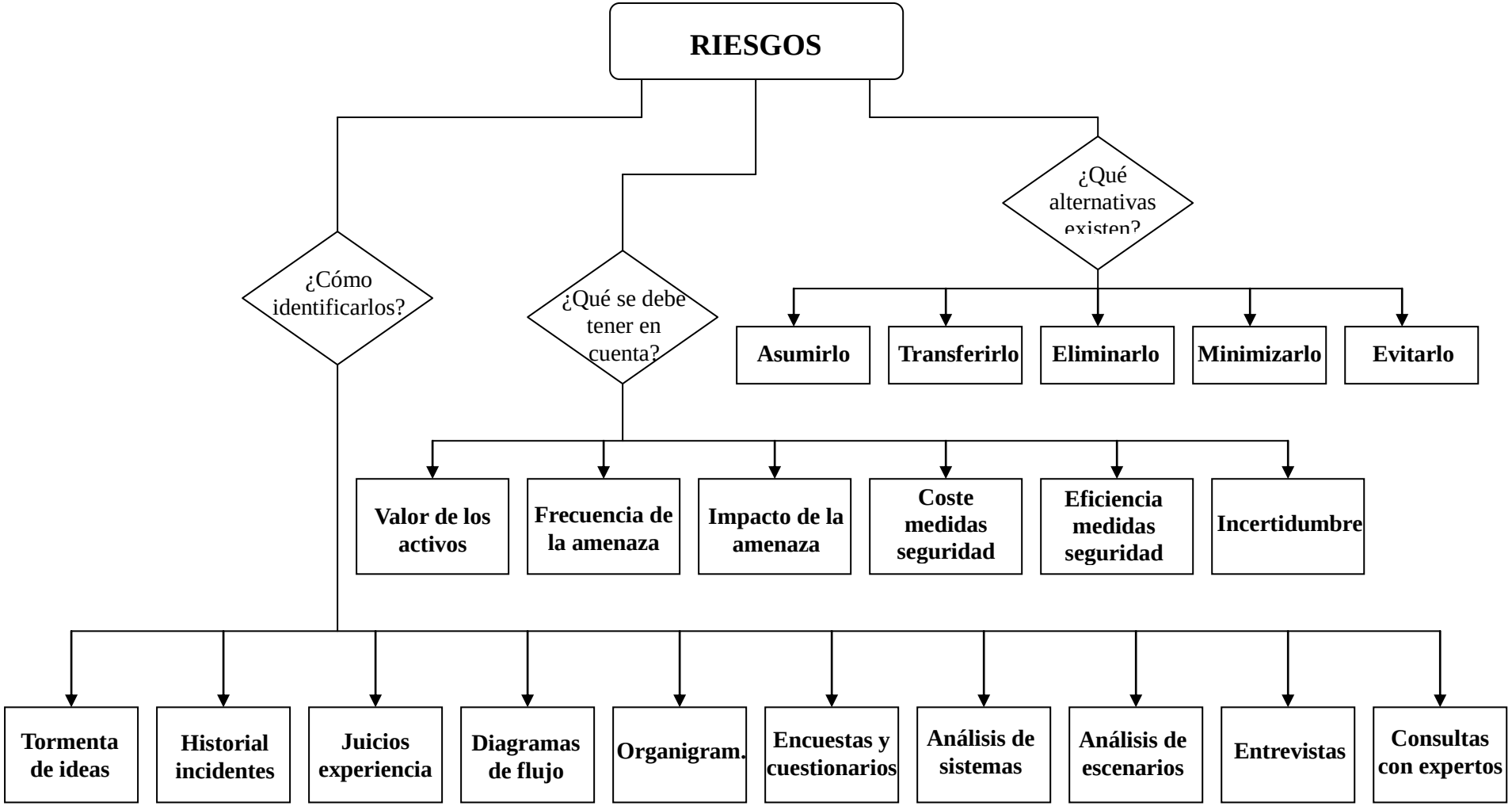


Figura 2.7 Riesgos



2. 4 Análisis de impacto

Un impacto es una consecuencia negativa que sufre la organización si las funciones que generan las operaciones se vieran interrumpidas por cualquier motivo. Se ha de contemplar el tiempo de recuperación permitido si ocurriese un desastre sin que tenga un gran impacto en la continuidad de la actividad de la compañía.

Existen daños que pueden producir un impacto en la compañía de forma más crítica y serán en los que haya que prestar mayor atención. Por ejemplo, no causa el mismo impacto que la máquina de café deje de funcionar durante un día que si se produce una interrupción en el Sistema de Información de la empresa.

El análisis de impacto pretende identificar las funciones críticas priorizando las estrategias de recuperación que podrían ser necesarias si se produjese una interrupción. Se debe volver a la normalidad lo antes posible ya que el tiempo es un factor que juega en contra de la entidad y cuanto más se tarde en subsanar el daño, peores serán las consecuencias.

2. 4. 1 Etapas del análisis de impacto

i. Se **definen los tipos de impacto** a considerar.

Los impactos pueden ser de varios tipos:

- ✓ De pérdida de rentabilidad
- ✓ Incremento de costes y/o gastos
- ✓ Peligro para las personas
- ✓ Impacto comercial
- ✓ Impacto en la imagen
- ✓ Impacto ambiental
- ✓ Impacto operacional
- ✓ Impacto jurídico

Dependiendo de estos factores hay que buscar un equilibrio entre las actividades de prevención y de recuperación teniendo en cuenta los costes financieros.

ii.Se **identifican las funciones críticas** de la organización y sus interdependencias.

Las funciones críticas son aquellas que su interrupción producen un impacto en la entidad. Para identificar las funciones críticas de la organización es conveniente utilizar cuestionarios normalizados.

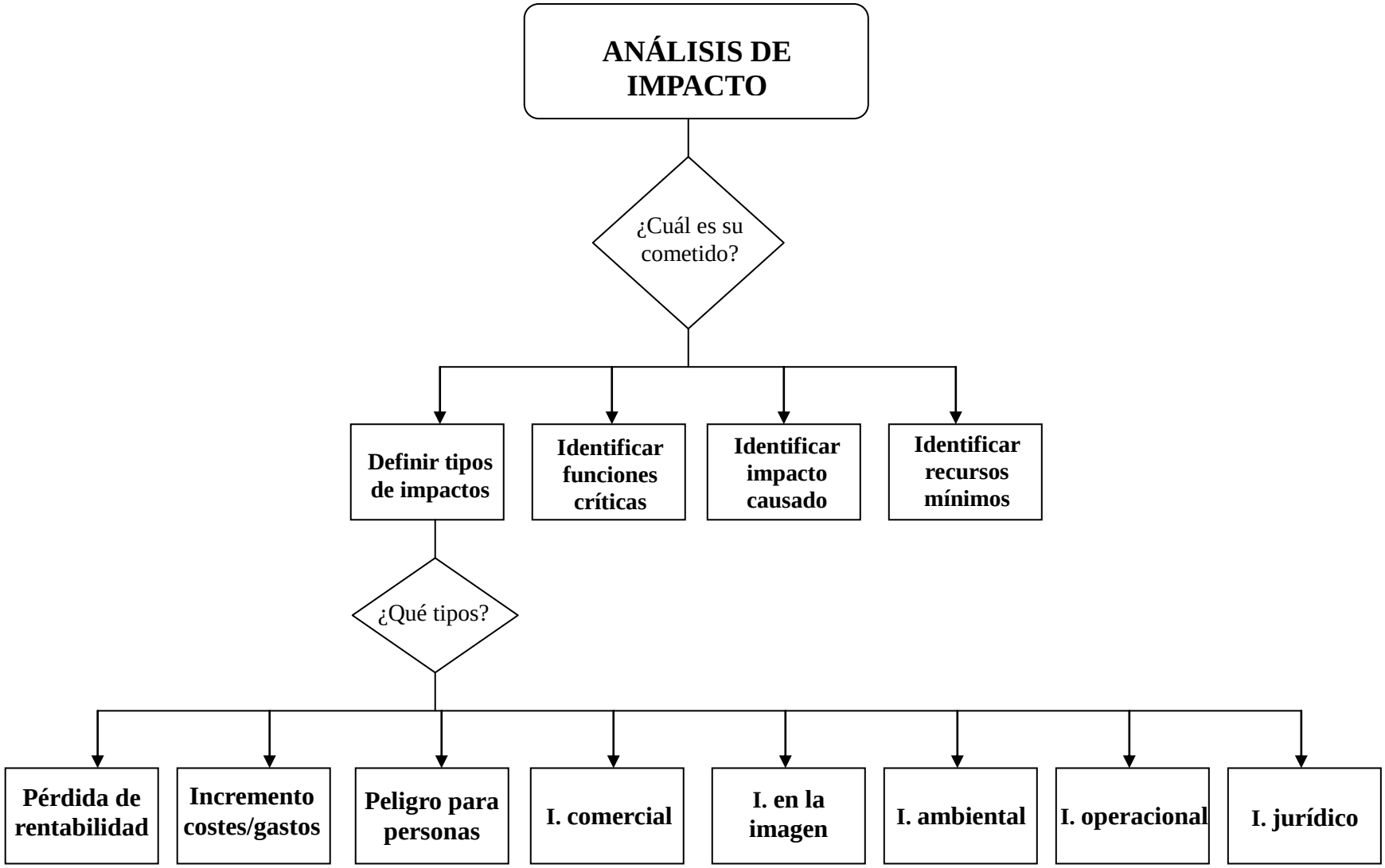
iii.Se **identifica el impacto causado** por la interrupción de cada función crítica.

Informar a la dirección de los resultados obtenidos para que priorice funciones dependiendo del grado de criticidad del impacto (tanto individual como en relación a otras funciones) que causaría la interrupción de cada una.

iv.Se **identifican los recursos mínimos** necesarios para la recuperación de las funciones.

Se asignan los recursos que son indispensables para dar soporte a la compañía en la recuperación de funciones.

Figura 2.8 Análisis de impacto



2. 5 Plan de Contingencias

El Diccionario de la Real Academia Española ofrece tres acepciones para definir **contingencia**: "*1. Posibilidad de que algo suceda o no suceda. 2. Cosa que puede suceder o no suceder. 3. Riesgo"*. De estas definiciones se deduce que un Plan de Contingencias pretenderá servir de guía de actuación ante una contingencia.

Un Plan de Contingencias es una descripción detallada de cómo se debe actuar ante determinados eventos que se produzcan, a fin de asegurar la continuidad del negocio. El plan ha de contener las medidas de índole técnica, organizativa y humana para reaccionar ante un desastre, ya sea accidental o deliberado reduciendo al máximo el impacto producido en la empresa.

Se busca minimizar el número de decisiones a tomar durante una contingencia. El plan pretende minimizar los daños que el incidente produzca en la compañía. Además, procura disminuir el tiempo de interrupción de los sistemas que se vieran afectados y facilitar la restauración del sistema en el menor tiempo posible. También brinda a los empleados unas normas de actuación frente a situaciones de emergencia.

Elaborar un Plan de Contingencias no es una tarea sencilla, ya que su desarrollo dependerá del tamaño de los sistemas, las aplicaciones que pueden verse afectadas, las interrelaciones entre éstas, las prioridades entre los elementos y los riesgos a los que se enfrentan. El plan debe probarse con cierta periodicidad y realizar las actualizaciones oportunas cuando sea necesario.

Un Plan de Contingencias se compone de tres planes:

- **Plan de respaldo**: guía detallada que contempla las medidas que se han de llevar a cabo **antes** de que se produzca el incidente. Por ejemplo, realizar copias de respaldo es una medida preventiva, ya que si se produjese la contingencia, la información ya estaría previamente salvaguardada.
- **Plan de emergencia**: especifica las normas de actuación que se llevarán a la práctica **durante** ocurre el desastre o inmediatamente después. Por ejemplo, restaurar las copias de seguridad de la información dañada o eliminada.
- **Plan de recuperación**: desarrolla las normas a seguir para retornar la actividad normal en la organización **después** de materializarse la amenaza. Por ejemplo, reparar o sustituir los elementos dañados durante la contingencia.

2. 5. 1 Fases de un Plan de Contingencias

El desarrollo del Plan de Contingencias podría dividirse en las siguientes fases:

- **Planificación**: Primeramente, se conciencia a la alta dirección de la necesidad de implementar un Plan de Contingencias. Se debe ayudar a la dirección a establecer factores críticos de éxito, alcance, políticas y objetivos del plan.

  Después se planifican los recursos técnicos, humanos y económicos que son necesarios para llevar a cabo el plan. El desarrollo de dicho plan no ha de ser un proyecto del Departamento de Informática solamente sino que debe participar toda la organización. Su elaboración debe plantearse como cualquier proyecto desarrollado en la compañía, marcando sus objetivos, etapas, tiempos, costes…

- **Análisis de riesgos y Análisis de impacto**: Se realiza un análisis de riesgos y de impactos (explicados en los apartados 2.3 y 2.4 de este capítulo).

- **Desarrollo de estrategias de continuidad**: después de determinar las funciones críticas (identificadas en el Análisis de impacto), se ha de estudiar la estrategia de recuperación de las funciones. También se establecen prioridades de recuperación.

  Dentro de las estrategias de continuidad, comentar que se debe contar con un centro de respaldo, es decir, un centro de procesamiento de datos (CPD) que tome el control de otro CPD principal en caso de que se produzca un desastre. El centro de respaldo deberá encontrarse alejado de aquél para no verse afectado también si se produce un incidente. Asimismo, deberá contar con el mismo equipamiento *software* (y mismas versiones) y un equipamiento *hardware* compatible con el del centro de procesamiento de datos principal.

  Además, es necesario disponer de los datos con los que se trabaja en el CPD original. Para ello, deben realizarse copias de seguridad que recuperen la información cuando se desencadena un desastre.

- **Desarrollo del Plan de Contingencias**: Se definen los procedimientos de recuperación en caso de que se produzca un incidente. Incluye las normas de actuación que se deban llevar a cabo antes, durante y después de la interrupción.

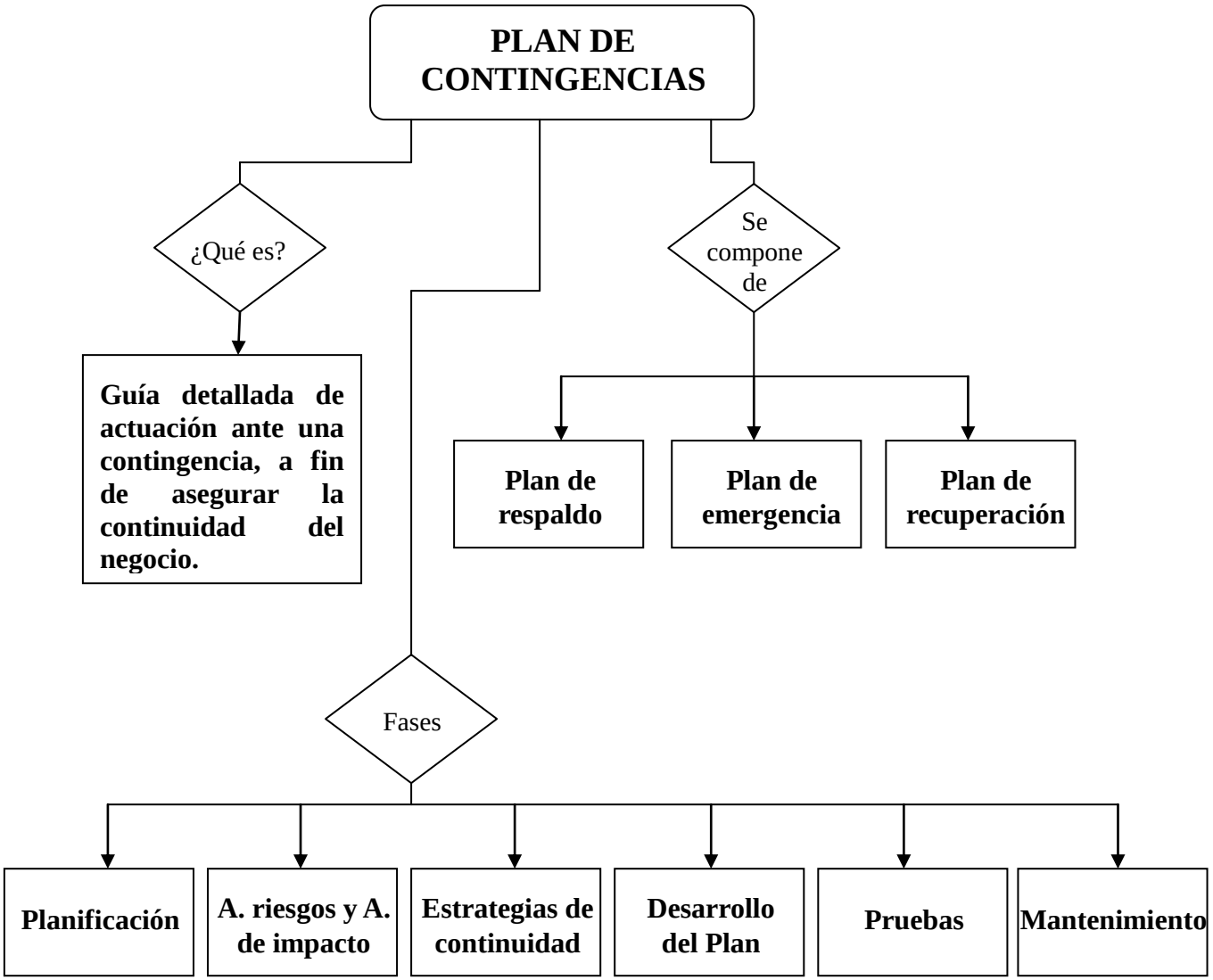
  El plan debe recoger los protocolos de actuación a seguir, los recursos materiales que han de utilizarse, expresar a quién va dirigido y cuales son las responsabilidades concretas de dichas personas.

  También se debe formar y entrenar al personal para que aprendan a actuar si se materializa una amenaza y saber como poner en marcha los procedimientos necesarios para evitar o reducir el desastre.

- **Pruebas**: Se efectúan las pruebas pertinentes para detectar las deficiencias y corregirlas. Las pruebas se repetirán con cierta periodicidad para asegurarse que el plan funciona correctamente.

- **Mantenimiento**: El plan conlleva un mantenimiento continuo y se modificará para adaptarse en todo momento a las necesidades de la organización y de los sistemas.

Figura 2.9 Plan de Contingencias



2. 6 Política de Seguridad

Las Políticas de Seguridad son pautas y procedimientos que proporcionan a la dirección soporte relativo a la seguridad conforme con los requisitos legales y de negocio. Para su existencia es necesario que exista un alto compromiso de la gerencia, quién se encargará además, de aprobar el documento.

El objetivo de la Política de Seguridad será que todo el personal de la empresa, desde el becario recién llegado al más alto cargo, asimile y cumpla las directrices marcadas en el documento para prevenir daños en la organización.

Asimismo, debe ser accesible y entendible por todo el personal de la compañía. Por esta razón, estará escrito en un lenguaje sencillo, evitando ambigüedades y tecnicismos. De nada sirve tener una política que no es comprensible a todos los niveles de la organización porque, entonces, no todos la podrán cumplir. Si la Política de Seguridad se suministra fuera de la empresa se tendrá especial cuidado en no facilitar datos confidenciales.

Para que sean eficientes y eficaces, las Políticas de Seguridad deben revisarse y actualizarse cada cierto tiempo o si ocurre algún hecho relevante que pudiera dar cabida a una modificación en el documento. Asimismo, la Política de Seguridad puede formar parte de la política general de la empresa.

En necesario que exista un responsable que se encargue del desarrollo de la Política de Seguridad, de su revisión y su evaluación. Esta persona tendrá los conocimientos suficientes de las actividades que se realizan en la empresa para poder desarrollar las medidas de seguridad oportunas y con la suficiente formación y experiencia para llevar a cabo dicha labor.

2. 6. 1 Elementos que conforman una Política de Seguridad

Los aspectos mínimos deducidos del Estándar Internacional ISO/IEC 17799 (actualmente denominada ISO/IEC 27002) que se requieren para realizar la Política de Seguridad son lo siguientes:

- Definición de la seguridad de la información, los objetivos y alcance de la política, y la importancia de la seguridad.
- Descripción de los objetivos y principios de la seguridad en concordancia con la estrategia y los objetivos comerciales de la compañía.
- Marco referencial para determinar los objetivos de control y los controles, y añadir la estructura de la evaluación y la gestión del riesgo.
- Una concisa exposición de las políticas, estándares y requerimientos de conformidad de la seguridad.
- Definición de las responsabilidades en la gestión de la seguridad de la información, adjuntando además, el reporte de incidentes de seguridad de la información.
- Alusión a la documentación que fundamenta la política.

2. 7 Mecanismos de Seguridad

Para implementar la Política de Seguridad se utilizan mecanismos de seguridad. La política define lo que se puede hacer y lo que no, y los controles de seguridad se encargan de hacer cumplir la política.

Los mecanismos de seguridad se dividen en tres grupos:

- ✓ De prevención
- ✓ De detección
- ✓ De recuperación

2. 7. 1 Mecanismos de prevención

Los mecanismos de prevención se llevan a cabo antes de que ocurra un incidente y su función es no permitir que suceda. Aumentan la seguridad del sistema bloqueando los accesos no autorizado.

Si se emplean controles de prevención muy completos no será necesario el uso excesivo de mecanismos de detección o recuperación. El mecanismo de prevención más importante es la concienciación de todos los empleados de la importancia de estos controles.

Se pueden distinguir los siguientes mecanismos de prevención: de autenticación e identificación, de control de accesos, de separación y de seguridad en las comunicaciones.

- **Mecanismos de autenticación e identificación**: Son mecanismos muy importantes que aseguran que sólo los usuarios autorizados puedan acceder al sistema y evita accesos ilegítimos. Además, estos controles aseguran que los usuarios sólo acceden a las áreas permitidas.

  Identificar y autenticar no es lo mismo. Según El Diccionario de la Real Academia Española, identificar es "*Reconocer si una persona o cosa es la misma que se supone o se busca*" y autenticar es "1. *Autorizar o legalizar* algo. 2. *Acreditar (// dar fe de la verdad de un hecho o documento con autoridad legal).*"

Existen tres categorías de métodos de autenticación para verificar la identidad de los individuos:

⇒ **Algo que el usuario conoce**: puede ser una contraseña, un dato acerca de su persona…

⇒ **Algo que la persona lleva consigo**: una tarjeta inteligente, una tarjeta de identidad…

⇒ **Característica física del individuo o acto involuntario de éste**: técnicas biométricas, una firma…

Los accesos a un sistema que pueden realizarse por medio de un identificador y una contraseña. Es recomendable que la identificación y autenticación se realice de forma individual, es decir, que varios usuarios no puedan acceder al sistema con el mismo identificador y contraseña.

Si algún individuo consigue apoderarse de la contraseña de un empleado puede causar mucho daño a la entidad. Para evitarlo, se debe seguir una serie de consejos:

- Primero, y aunque sea obvio para muchas personas, nunca se ha de guardar las contraseñas en un archivo del ordenador, escribirlas en un pósit a la vista de todos o facilitárselas a terceros en un exceso de confianza.
- En ocasiones, nos facilitan contraseñas por defecto, las cuales no las cambiamos por pereza. Debemos sustituirlas en cuanto sea posible.
- Evitar el uso de secuencias lógicas, nombres, teléfonos o fechas señaladas cuando creamos la contraseña.
- Una *password* segura debe contener: mayúsculas, minúsculas, letras, números y signos de puntuación.
- La longitud mínima aceptable es de ocho caracteres, aunque lo ideal sería a partir de catorce.
- Deben cambiarse con frecuencia. Lo ideal es cambiar las contraseñas, al menos, cada 30 días o si se sospecha que se han podido dejar de ser confidenciales.
- Evitar el uso de contraseñas ya usadas anteriormente para identificarse en el sistema.

- Por último, evitar el uso de la misma contraseña para distintos sistemas.

También existen otras formas de identificación a través de tecnologías de biometría, Kerberos, criptografía, firma electrónica, tarjetas con bandas magnéticas, tarjetas inteligentes, entre otras. A continuación, se explican algunos elementos de identificación:

- **Criptografía**: consiste en cifrar o descifrar información permitiendo que sea incomprensible para cualquier agente externo al mensaje. Permite la confidencialidad de la información y, en muchas ocasiones, también la integridad.

  Se pueden utilizar algoritmos de clave simétrica o de clave asimétrica:

  - Los algoritmos de **clave simétrica**, también llamados de clave **privada**, utilizan la misma clave para cifrar y descifrar el mensaje. El remitente y el destinatario eligen la clave a utilizar antes del envío de mensajes.

    Algunos algoritmos de clave simétrica son: DES (*Data Encryption Standard*), Triple DES (variante del algoritmo DES) y AES (*Advanced Encryption Standard*).

  - Los algoritmos de **clave asimétrica**, o denominados de clave **pública**, emplean una clave para cifrar y otra clave distinta para descifrar. Cada persona posee un par de claves, una clave pública que entregan a cualquier otra persona y la otra clave privada que solo conoce el propietario.

    El remitente puede emplear la clave pública del destinatario para cifrar el mensaje y el receptor con su clave privada lo descifra. Si el remitente usa su clave privada para cifrar el mensaje, cualquier persona puede descifrarlo utilizando su clave pública. Existen varios algoritmos de clave asimétrica como RSA o Diffie-Hellman.

- **Firma electrónica**: es un conjunto de datos en forma electrónica, que se añaden a otros datos para identificar formalmente al firmante del documento. La firma electrónica está basada en la criptografía de clase asimétrica.

  Si además, la firma electrónica permite revelar cualquier modificación de los datos firmados, es decir, garantiza la integridad de los datos, se denomina **firma electrónica avanzada**. Por lo tanto, permite autenticar a la persona que envía el mensaje, garantizar la integridad de la información e implica que el firmante no pueda repudiar su participación.

  Los prestadores de servicios de certificación permiten el empleo de firma electrónica mediante la expedición de certificados electrónicos. Una clase particular de certificados electrónicos son los certificados reconocidos.

  Si la firma electrónica está basada en un certificado reconocido y se crea bajo un dispositivo seguro de creación de firma se denomina **firma electrónica reconocida**. Este tipo de firma se equipara a funcionalmente con la firma manuscrita.

  La firma electrónica se regula en España por la Ley 59/2003, de 19 de diciembre, de firma electrónica.

- **Kerberos**: protocolo de seguridad que permite que en una red no segura dos ordenadores demuestren su identidad recíprocamente de forma fiable usando criptografía de clave simétrica. Evita tener que enviar contraseñas a través de la red y que usuarios no autorizados las intercepten.

  Kerberos tiene una base de datos con todas las contraseñas de los usuarios y de los servidores. La clave de cada usuario está cifrada y procede de su contraseña, y en el caso del servidor, la clave se genera aleatoriamente. Los usuarios al igual que los servicios de red que soliciten, se deben registrar en Kerberos.

Las claves privadas son negociadas cuando los usuarios se registran. Además, como Kerberos conoce todas las claves privadas, informa a los servidores, a través de mensajes, de la autenticidad de los usuarios que solicitan sus servicios.

Requiere un tercero de confianza, denominado "centro de distribución de claves" (KDC, *Key Distribution Center*) que consta de: un servidor de autenticación "AS" (*Authentication Server*) y un servidor para facilitar *tickets* "TGS" (*Ticket Granting Server*). El usuario es autenticado y se le entrega un ticket para comunicarse con el servidor de tickets, el cual suministra las credenciales que el usuario necesita para comunicar con el servidor que le ofrece el servicio.

En la arquitectura de Kerberos se distinguen tres objetos de seguridad: la clave de sesión, el ticket y el autenticador.

- Clave de sesión: clave generada por Kerberos que es proporcionada a un usuario para usarla en un servidor durante una sesión.
- *Ticket*: testigo que se proporciona a un usuario para solicitar los servicios de un servidor. Garantiza que el usuario ya ha sido autenticado anteriormente.
- Autenticador: testigo enviado a un servidor para probar la identidad del usuario. Es posible utilizarlo sólo una vez.

❖ **Tecnologías de identificación biométricas**: digitalizan y almacenan algún rasgo físico o del comportamiento humano para su identificación. Para verificar la entidad de personas es necesario que sus rasgos biométricos se comparen con el patrón ya guardado de antemano, es decir, una persona que sus características no estén almacenadas en el sistema no podrá ser autenticada.

El indicador biométrico que analiza algún rasgo de la persona debe tener las siguientes características:

- Universalidad: Todas las personas poseen ese rasgo.
- Unicidad: La probabilidad de encontrar dos personas con una característica idéntica es mínima.
- Cuantificación: El rasgo puede ser medido de manera cuantitativa.
- Permanencia: La característica no varía con el paso del tiempo.

Existen varias técnicas biométricas:

- ✓ Patrones faciales
- ✓ Huellas dactilares
- ✓ Termografía facial
- ✓ Patrones de la retina
- ✓ Reconocimiento de voz
- ✓ Reconocimiento del iris
- ✓ Geometría de la palma de la mano

❖ **Tarjetas con bandas magnéticas**: Son tarjetas que tienen una banda magnética, negra o marrón, que identifican a través de señales electromagnéticas de alta o baja energía que se registran y codifican información en bandas. Es una opción sencilla para controlar el acceso a edificios o zonas privilegiadas y tiene un coste bastante bajo.

En el control con tarjetas magnéticas se distinguen cuatro elementos importantes: un sistema de grabación y codificación de la banda magnética, un sistema de impresión y caracterización de las tarjetas, un programa de gestión de entradas y/o salidas y lectores de banda magnética.

- **Tarjetas inteligentes**: Son tarjetas de plástico que llevan adheridas un circuito integrado que almacena y procesa datos confidenciales. Pueden modificar su contenido sin la necesidad de un grabador demasiado caro.

  Además, se puede realizar múltiples grabaciones sin que exista riesgo de perder la información. Debido a su almacenamiento más seguro y mayor espacio de memoria, están remplazando a las tarjetas de banda magnética. Los lectores de tarjetas son los que proporcionan la energía, razón por la cual, las tarjetas inteligentes carecen de baterías.

  Se distinguen dos grupos de tarjetas inteligentes:

  - Tarjetas microprocesadas: Generalmente no almacenan gran cantidad de datos. Contienen una zona de memoria "protegida" a la que sólo puede acceder su fabricante garantizando una identificación única a nivel universal. Se usan bastante en la banca.
  - Tarjetas de memoria: Almacenan mayor cantidad de información. Son totalmente grabables por lo que no garantizan plenamente la identificación y debido a esto, se utilizan sistemas de cifrado propios de la aplicación con la que opera la tarjeta.

  Para leer tarjetas inteligentes pueden utilizarse lectoras universales, que leen más de un tipo de tarjeta, lo que conlleva un precio elevado, o especializadas, que leen pocos tipos de tarjetas pero son más económicas.

  Entre las aplicaciones que tienen estas tarjetas inteligentes destacan la de identificación, control de acceso y de presencia que limitan y controlan el acceso a edificios, áreas restringidas, oficinas, ordenadores, aplicaciones, bases de datos, ficheros, redes…

- **Mecanismos de control de acceso**: Verifican que sólo accedan a las áreas y recursos de la entidad los individuos que estén autorizados. Limitan y controlan el acceso detectando el número de intentos y evitando el acceso de intrusos.

  Para llevar a cabo estos controles, la organización debe primero identificar y autenticar a los sujetos, para que los derechos de acceso sean acordes a cada individuo. Por tanto, estos controles de acceso están muy ligados con los mecanismos de autenticación e identificación.

- **Mecanismos de separación**: Separa los objetos en cada nivel e impide que objetos y entidades de distintos niveles se comuniquen si no existe autorización por parte de los mecanismos de control de acceso.

  Según la forma de separar los objetos se puede distinguir cinco grupos:

  - ✓ Separación lógica
  - ✓ Separación física
  - ✓ Separación temporal
  - ✓ Separación criptográfica
  - ✓ Separación de fragmentación

- **Mecanismos de seguridad en las comunicaciones**: Protege la integridad y la confidencialidad de los datos en las comunicaciones. Para evitar ataques en el intercambio de datos, debe cifrarse la información.

2. 7. 2 Mecanismos de detección

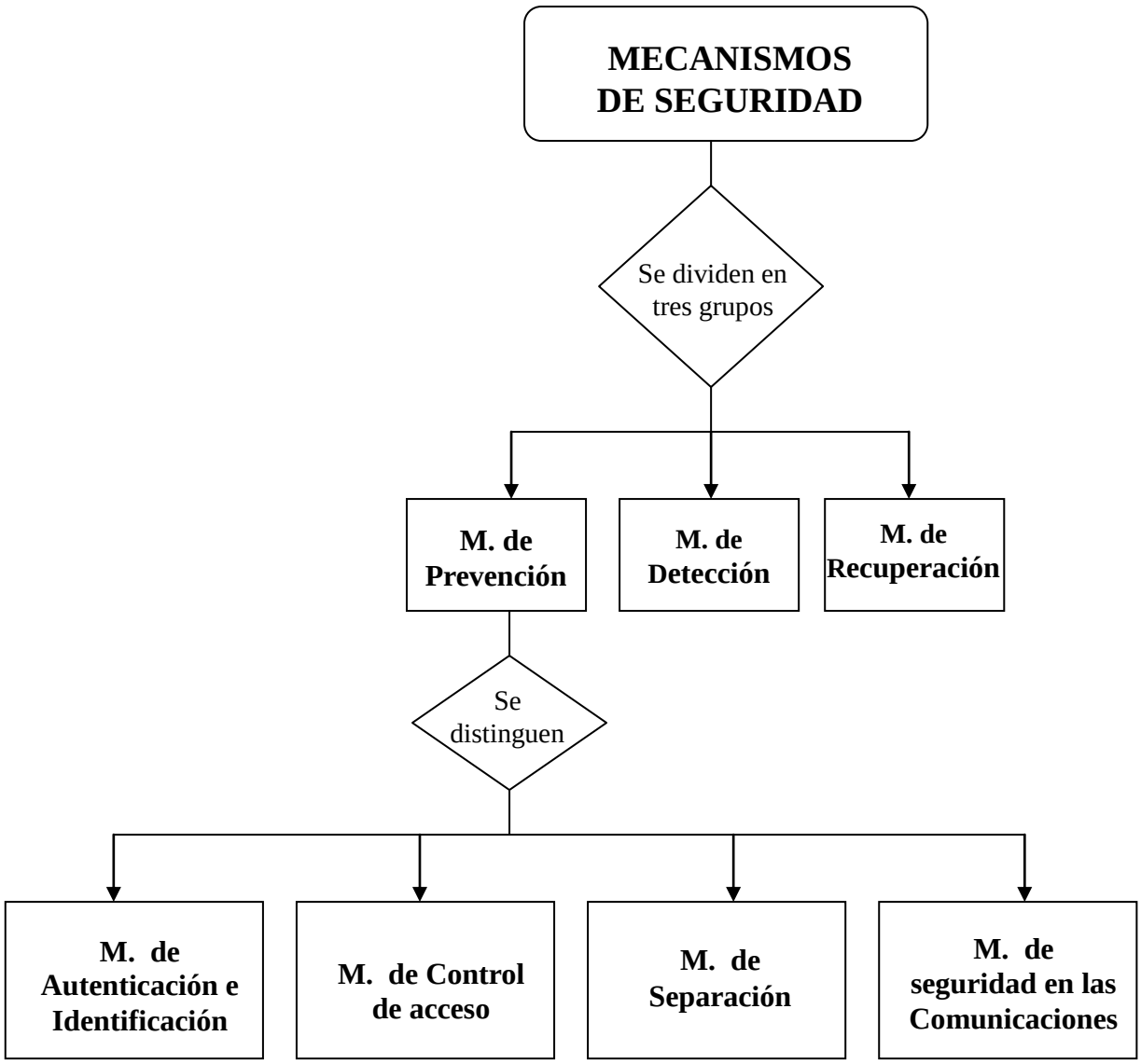
Los mecanismos de detección revelan violaciones (o intentos de violación) de la seguridad. Un programa como *Tripwire* ayuda a detectar cambios en el sistema. *Tripwire* es una herramienta que monitoriza y avisa de cambios realizados asegurando la integridad de la información almacenada en los ficheros. Es recomendable instalarlo antes de que el ordenador haya tenido acceso a Internet.

2. 7. 3 Mecanismos de recuperación

Se llevan a cabo cuando ya se ha producido una violación en el sistema, e intentan que retorne a su estado normal. Dentro de este tipo de controles existe un conjunto denominado mecanismos de análisis forense que, además de procurar reanudar al sistema a su estado normal, investiga el alcance de la violación, la forma en la que se ha producido para solucionarlo y las actividades que ha llevado a cabo el intruso.

Tras un daño producido en el sistema es posible revertir la información a su estado original por medio de copias de seguridad. Es imprescindible que el mecanismo de copia de seguridad que se implemente esté diseñado de forma que asegure la recuperación y la continuidad de toda la información importante de la empresa, sin interrumpir la actividad del sistema.

Figura 2.10 Mecanismos de seguridad



III. SEGURIDAD LÓGICA

3. 1 Introducción

La seguridad puede dividirse, a grandes rasgos, en dos grandes bloques: seguridad física y seguridad lógica. Para salvaguardar los activos de la empresa no puede existir una sin la otra, ambas son complementarias. De nada sirve controlar los accesos físicos a las instalaciones para no sufrir percances y mantener a salvo los bienes, si un individuo puede acceder a la información confidencial de la compañía cómodamente desde el ordenador de su casa.

En el capítulo anterior, se abordó brevemente el tema de la seguridad física cuyo término hace referencia a la protección de la organización frente a accesos no autorizados y ataques físicos a los ordenadores, instalaciones, personal, documentación, etc. En las próximas páginas se expondrá el otro bloque importante, la seguridad lógica, la cual garantiza la seguridad a nivel de los datos, permitiendo el acceso lógico a la información sólo a personas autorizadas.

La seguridad lógica aplica mecanismos y barreras que mantengan a salvo la información de la organización desde su propio medio. Algunos de los controles utilizados en la seguridad lógica son:

- ⇒ Se limita el acceso a determinados aplicaciones, programas o archivos mediante claves o a través de la criptografía.
- ⇒ Se otorgan los privilegios mínimos a los usuarios del sistema informático. Es decir, sólo se conceden los privilegios que el personal necesita para desempeñar su actividad.
- ⇒ Cerciorarse de los archivos, las aplicaciones y programas que se utilizan en la compañía se adaptan a las necesidades y se usan de manera adecuada por los empleados.
- ⇒ Controlar que la información que entra o sale de la empresa es íntegra y sólo esta disponible para los usuarios autorizados.

A lo largo de este capítulo se reflejarán muchos de los peligros a los que se enfrentan nuestras empresas desde el punto de vista de la seguridad lógica. Seguramente, en los próximos años surjan nuevas amenazas que deberán ser estudiadas para evitar sus consecuencias y actuar ante su posible aparición, al igual que las detalladas en este documento.

3. 2 Subestados de la seguridad de la información

Los subestados o atributos de la seguridad de la información, también conocidos como requisitos **ACID** (autenticación, confidencialidad, integridad y disponibilidad), son los siguientes:

- **Autenticación**: Garantiza que el usuario es "quien dice ser".
- **Confidencialidad**: La información sólo se revela a los usuarios autorizados para prevenir el acceso no autorizado, ya sea de manera intencional o accidental.
- **Integridad**: La información debe ser siempre exacta y completa, y sólo puede ser modificada por personal autorizado.
- **Disponibilidad**: La información sólo ha de estar disponible cuando se necesite y de la forma que la requieran los usuarios autorizados.

Además, se pueden considerar otros aspectos adicionales a de seguridad:

- **No repudio**: Es una manera de asegurar que ninguna de las partes involucradas pueda negar su participación. Característica importante en el comercio electrónico y banca.
- **Trazabilidad**: permite asociar acciones realizadas en un sistema con el individuo o sistema que las llevó a cabo y en qué momento.

3. 3 Amenazas lógicas

Para evitar posibles amenazas lógicas en nuestra organización, es importante que todos los empleados, especialmente los administradores de los equipos, tomen conciencia del cuidado que deben poner para que no se materialicen posibles daños en la compañía.

Además, es fundamental implementar mecanismos de prevención, detección y recuperación ante posibles amenazas lógicas como virus, gusanos, bombas lógicas y otros códigos maliciosos.

La expansión de la cultura de la seguridad entre los empleados puede ahorrar muchos disgustos a la entidad, muchas veces implementando medidas tan sencillas como, por ejemplo:

- No ejecutar programas de los que se desconozcan su procedencia.
- No utilizar programas no autorizados por la dirección.
- No abrir correos personales desde los equipos de la compañía.
- No visitar páginas web que no sean propósito de la empresa.
- Instalar y actualizar habitualmente un *software* dedicado detectar y eliminar códigos maliciosos que puedan albergar los ordenadores.
- Realizar chequeos de los correos electrónicos recibidos para comprobar que no suponen una amenaza para la entidad.

El Estándar Internacional ISO/IEC 17799 versión 2005 (actualmente conocido como ISO/IEC 27002) recomienda que para protegerse de las amenazas lógicas, la empresa debe contar con dos o más programas (procedentes de diferentes vendedores) encargados de detectar y reparar códigos malicioso para mejorar las probabilidades de éxito ante un ataque.

Éstas y otras medidas facilitarán el buen funcionamiento de la organización. A continuación, se detallan las amenazas lógicas más frecuentes que pueden dañar los bienes de la empresa y las posibles formas de evitar o disminuir la probabilidad de ocurrencia y el impacto que causaría en la entidad.

3. 3. 1 *Malware*

Un *malware* es todo *software* diseñado para realizar acciones maliciosas sobre el sistema. La palabra *malware* proviene del inglés "***mal****icious soft****ware***", es decir *software* malicioso o también llamado *badware*.

Existen gran cantidad de *malware* y seguramente aparecerán nuevos tipos, según evolucionen las nuevas tecnologías. En los sucesivos apartados se detallarán los *badware* más relevantes:

- Virus
- Gusanos

- Troyanos
- Bombas lógicas
- *Adware*
- *Spyware*
- Puertas traseras
- Conejo o bacteria
- *Rootkit*
- *Exploit*
- *Cookie*
- *Pharming*
- *Spam*

3. 3. 1. 1 Virus

Un virus es una secuencia de código que se aloja en un fichero ejecutable denominado *host* (huésped) de manera que al ejecutar el programa también se ejecuta el virus. Llevan a cabo diversas acciones que interfieren en el correcto funcionamiento del ordenador sin conocimiento del usuario.

Los virus informáticos son muy habituales en la red y pueden provocar daños irreparables. En algunas ocasiones, borran información necesaria para el correcto funcionamiento del sistema, y esto provoca que el disco duro tenga que ser formateado para reparar el daño. Ocupan poco espacio en disco, característica importante para que el virus pueda pasar inadvertido el máximo tiempo posible. Se auto-replican, es decir, se realizan copias de sí mismo para expandirse rápidamente.

El ciclo de vida de un virus es el siguiente:

⇒ El virus es programado.

⇒ Se expande.

⇒ Realiza la función maliciosa para la que está programado.

⇒ Finalmente, pueden ocurrir dos cosas: se produce su extinción o se produce una mutación. En este último caso, se repite el ciclo.

Los virus se pueden agrupar en dos tipos:

- Virus benignos: estos virus están programados para molestar al usuario pero no dañan al sistema.
- Virus malignos: causan algún tipo de daño en el sistema.

Es posible distinguir tres módulos en los virus informáticos:

- Módulo de reproducción: Maneja las rutinas para infectar a las entidades ejecutables procurando que el virus pase desapercibido a los ojos del usuario y, de esta forma, infectar otras entidades que cuando se ejecutan en otros ordenadores se consigue que el virus se propagarse rápidamente.
- Módulo de ataque: Contiene las rutinas de daño adicional. Este módulo, se activa con determinados eventos en el sistema como, por ejemplo, una fecha, una hora, si se encuentra un archivo determinado o lo que el programador del virus decidiera atacar.
- Módulo de defensa: Las rutinas de este módulo se encargan de proteger al virus e intentar que pase desapercibido el mayor tiempo posible.

Además, cabe destacar que existen varios tipos de virus según su manera de ejecutarse o su función. Podrían señalarse los siguientes:

- **Virus de archivo**: Infectan archivos con extensiones “.exe”, “.dll”, “.com”, “.ovl”, “.drv”, “.sys” y “.bin”. Cuando se ejecuta el archivo, el virus se activa y realiza la acción para la que ha sido programado.
- **Virus de enlace**: Modifican las direcciones, no permitiendo así, el acceso a los archivos. De esta forma, no es posible localizarlos y realizar acciones sobre ellos.
- **Virus de sobrescritura**: Sobrescriben archivos, eliminando los datos originales contenidos en los mismos.

- **Virus de macro**: Infectan documentos de determinadas aplicaciones como Word, PowerPoint, Excel, Access… La infección comienza al cargarse el documento. La aplicación, además del documento, también carga las macros que lo acompañan. Las macros son un conjunto de instrucciones que se ejecutan de manera secuencial mediante una sola llamada y permite la automatización de tareas repetitivas.

  La aplicación ejecuta las macros, las cuales se hacen con el control del sistema por unos instantes. Entonces se copian al disco duro y modifican la plantilla maestra para que sean ejecutadas al iniciar la aplicación. Si los documentos infectados son abiertos en otro ordenador se propaga la infección.

- **Virus de *boot***: Infectan el *Master Boot Record* en el sector de arranque o el *Disk Boot Record* existente en los discos duros y disquetes. Los virus de *boot* sustituyen el código de arranque por otro y se propagan cuando se inserta un disco infectado en la unidad de arranque y se enciende el ordenador. De esta forma, se propaga el virus cargándose cada vez que se arranque el equipo. También reciben el nombre de virus de arranque.

- **Virus residentes**: Se insertan en la memoria del ordenador y permanecen en ella a la espera de que se ejecute algún programa o se utilice algún archivo para actuar.

- **Virus de acción directa**: Su función es opuesta a la de los virus residentes. Infectan los ordenadores en cuanto se ejecutan y realizan las acciones maliciosas para las que estén programados.

- **Virus mutantes**: Varían fragmentos de código fuente dificultando así su detección y extinción. También reciben el nombre de virus polimórficos.

- **Virus falso o *hoax***: En realidad, no se trata de virus sino cadenas de mensajes propagados por correo electrónico y redes. En general, informan sobre virus que en la mayoría de los casos son inexistentes para sobrecargar el flujo de información.

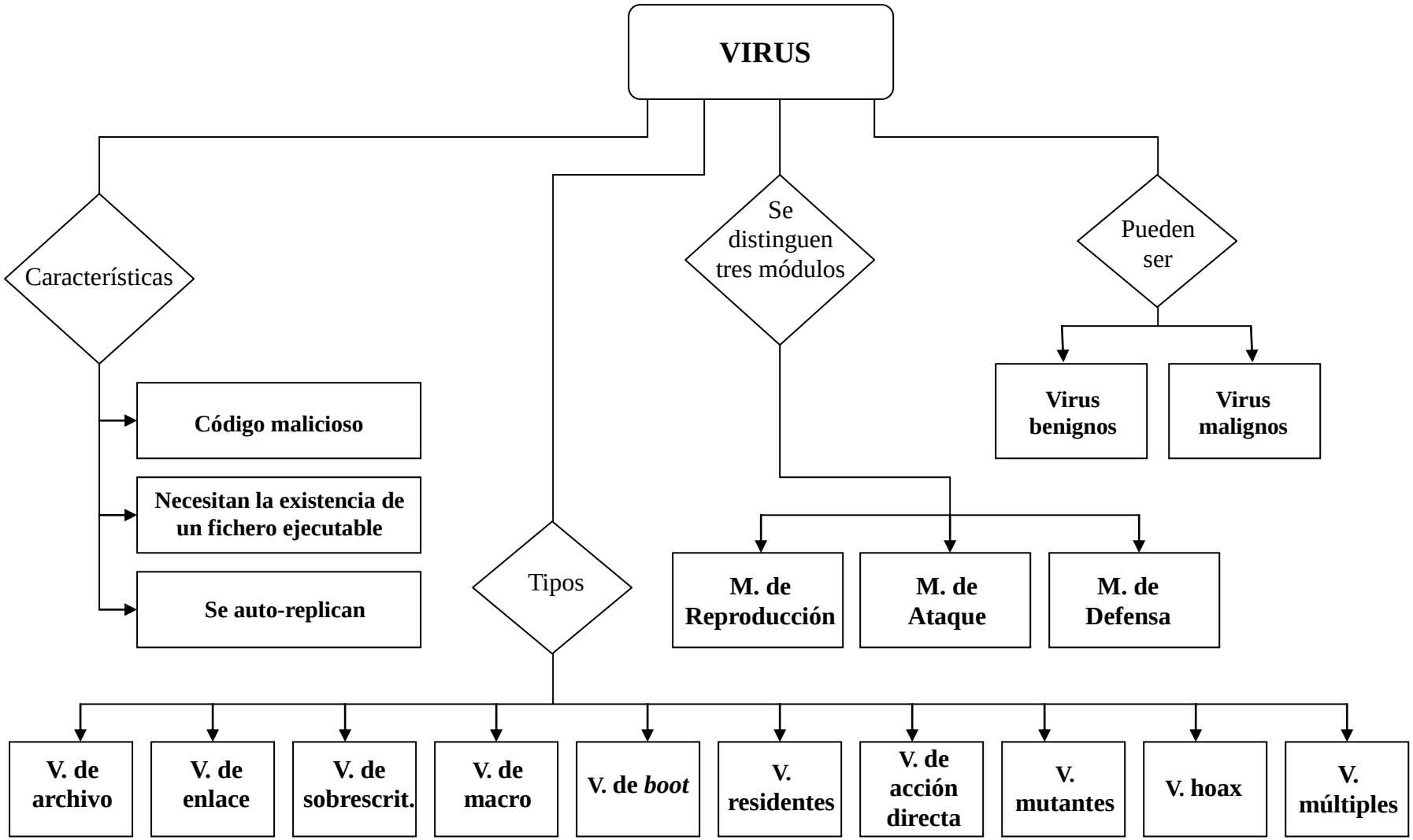
- **Virus múltiples**: Infectan archivos ejecutables y sectores de arranque simultáneamente, combinando la acción de los virus de archivo y de los virus *boot*.

Los virus necesitan de la existencia de otro programa para poder ejecutarse. Para protegernos de estos fragmentos de programa maliciosos es vital contar con un buen antivirus y mantenerlo siempre actualizado.

Uno de los primeros virus informáticos que se propagaron fue *Creeper* (enredadera en castellano) en 1971, difundido en la red ARPANET. Mostraba el siguiente mensaje: "*I'm the creeper, catch me if you can!*" lo que en castellano se podría traducir como "¡Soy una enredadera, atrápame si puedes!". Por suerte, no era un virus demasiado peligroso pero sí dio a conocer los agujeros de seguridad existentes en el *software* de las computadoras. Al poco tiempo, se creó *Reaper* (cosechadora) cuya misión era detectar y eliminar el virus "*Creeper*".

Michelangelo es otro virus informático que en 1992 se extendió por ordenadores de todo el mundo. Era un virus muy dañino que infectaba el sector de *boot* y el *Master Boot Record*. Se manifestó el 6 de marzo de 1992, sobrescribiendo información importante del disco duro.

Figura 3.1 Virus



3. 3. 1. 2 Gusanos

En inglés, el término que se utiliza es w*orm*. Los gusanos son programas capaces de ejecutarse por sí mismos (a diferencia de los virus que necesitan de la existencia de un fichero ejecutable) y propagarse por la red. A día de hoy, constituyen una amenaza habitual en Internet y las consecuencias que conllevan pueden ser fatales.

Se consideran como una subclase de virus informático. Residen en memoria y tiene gran capacidad para replicarse pudiendo incluso, enviar copias de sí mismo a otros equipos por medio de correos electrónicos. Es frecuente detectar que nuestro ordenador está infectado con un gusano cuando los recursos del sistema se consumen y detectamos que la máquina desempeña su actividad muy lentamente. Esto es debido a que el gusano se auto-replica y envía copias a otros ordenadores a través de las redes de comunicación sin intervención de ningún usuario.

El primer gusano llamado *Morris* apareció en noviembre de1988 y se estima que afectó a 6.000 servidores (aproximadamente el 10% de los servidores existentes en aquella época). Este gusano enviaba duplicados ilimitados de sí mismo a través de correos electrónicos sobrecargando las redes. Además de enviarse a otras máquinas a través de ARPANET, se duplicaba en los equipos infectados.

Los gusanos utilizan técnicas para aprovecharse del comportamiento humano y conseguir propagarse. Esto es lo que se denomina **ingeniería social**. Se utiliza con frecuencia en el caso de gusanos que se envían a través de *mails*.

Un ejemplo de gusano muy conocido que utiliza la ingeniería social y se propagaba a través de correos electrónicos es "*I Love You*". Este *worm* ha traído de cabeza a muchos usuarios. Se propagaba a través de correos electrónicos utilizando como asunto el nombre que le asignaron, que en castellano se traduce como "Te quiero". En él, se adjuntaba un archivo denominado "LOVE-LETTER-FOR-YOU.TXT.vbs" ("Carta de amor para ti"). "*I Love You*" logró engañar a muchas personas de todo el mundo creyendo que lo que recibían verdaderamente era una carta de amor. Apareció en marzo del año 2000 e infectó más de cincuenta millones de ordenadores.

Otro gusano que cabe mencionar es "*Blaster*". Fue detectado en el año 2003 y sólo atacaba a ordenadores con sistema operativo Windows 2000/2003/XP/NT. Aprovecha vulnerabilidades en los servicios de RPC (procedimientos de llamadas remotas) para propagarse a otras máquinas. Muestra los siguientes mensajes: "*I just want to say LOVE YOU SAN!!*" ("¡Sólo quiero decir que te amo San!") y "*billy gates why do you make this possible? Stop making money and fix your software!!"* ("Billy Gates, ¿por qué haces esto posible?, ¡deja de hacer dinero y arregla tu *software*!").

3. 3. 1. 3 Troyanos

Un caballo de Troya o troyano es un programa que bajo una apariencia inofensiva y útil para el usuario se inserta en un ordenador, y permite que usuarios externos accedan a la información contenida o controlen de forma remota el equipo. Los troyanos son creados para obtener información privilegiada de la máquina anfitriona. No necesariamente provocan daños en la computadora infectada y, a diferencia de los virus y los gusanos, los troyanos no se reproducen.

El nombre de Caballo de Troya proviene de la Guerra de Troya en la que según cuenta la historia, los griegos regalaron a la ciudad de Troya un caballo de madera como señal de paz después de una larga guerra. La ciudad estaba amurallada y hubo que derribar parte de esos muros para introducir el caballo debido a sus enormes dimensiones. Una vez dentro, al caer la noche, del caballo emergieron soldados que abrieron las puertas de la ciudad para que entraran los invasores griegos y destrozaran Troya.

Generalmente los caballos de Troya son utilizados para espiar, instalando en la máquina anfitriona un *software* de acceso remoto para observar las actividades que realiza el usuario del ordenador. Estos troyanos reciben el nombre de programa espía o *spyware*. Si lo que se pretende es capturar secuencias insertadas en el teclado para conseguir contraseñas reciben el nombre de *keylogger*. También existen troyanos que pueden abrir puertas traseras al ordenador para que un tercero realice las acciones maliciosas que persiga.

Los troyanos se componen de dos programas: uno que envía las acciones que deben realizarse en la computadora anfitriona llamado cliente, y otro programa que recibe las acciones del cliente y las realice desde el ordenador infectado denominado servidor. Algunos troyanos incluyen un archivo secundario con extensión ".dll" llamado librería, necesario para que el troyano funcione. Otros, además, incluyen *EditServer* que permite personalizar el servidor de forma que el atacante realice las actividades que desee sobre el equipo infectado.

Los troyanos actuales constituyen una gran amenaza para los usuarios debido a que pasan bastante desapercibidos. Esto se debe a que el programa servidor no consume apenas recursos. Cuando se arranca el equipo, el caballo de Troya se ejecuta automáticamente y reside en memoria. A partir de ahí, puede esperar a que el usuario del ordenador infectado introduzca números de tarjeta de crédito, contraseñas de su correo electrónico, etc.

Nuestra organización podría infectarse con un troyano fácilmente si no se ponen los medios para evitarlo. Un empleado podría recibir un correo electrónico con un archivo adjunto denominado "conferencia.avi" y al abrirlo ejecutarse el archivo con la extensión ".avi" y además, el troyano. Esto se debe a que un caballo de Troya puede ser incorporado en un fichero que cuando el usuario lo ejecuta, ambos archivos (el troyano y el archivo al que se adhiere) funcionan. De este modo, la persona que ha recibido el troyano no se da cuenta que en su computadora se ha instalado un programa malicioso ya que el archivo que deseaba ejecutar ha funcionado correctamente.

Otra forma de infectar un ordenador consiste en enviar el servidor del troyano a la máquina que se desea infectar disfrazado en un archivo con una extensión doble. Un trabajador de la compañía podría recibir en su buzón de correo un archivo que a sus ojos se denomina "conferencia.avi" pero realmente el ordenador no muestra la verdadera extensión "conferencia.avi.exe". Al ejecutar el archivo, el usuario se da cuenta que el archivo que ejecuta no funciona y se instala el troyano.

Algunos troyanos a mencionar son *NetBus* y *BackOrifice*. Ambos se arrancan de forma automática cuando se inicia Windows. Uno y otro abren puertas traseras en un ordenador cuyo sistema operativo sea Windows 95/98 (*NetBus* también actúa en Windows NT). Además, *BackOrifice*, a diferencia de *NetBus*, cifra la comunicación entre el programa cliente y el de servidor.

Para evitar que nuestros ordenadores se infecten de troyanos, no debemos ejecutar ningún programa ni fichero ejecutable del que se desconozca el origen, además de contar con un antivirus actualizado y un *software* anti-troyanos.

3. 3. 1. 4 Bombas lógicas

Las bombas lógicas son programas que se activan después de cierto tiempo causando daños en el sistema. Es muy común en empleados descontentos que abandonan una empresa (por ejemplo, porque han sido despedidos o han decidido trabajar para la competencia) e introducen una bomba lógica en los ordenadores de la organización con el fin de que cuando se cumplan unas condiciones que el individuo haya establecido, la bomba lógica se active y cause algún tipo de daño en el sistema.

Por ejemplo, un proveedor de una aplicación *software* podría añadir al programa una bomba lógica para asegurarse de que si el cliente no realiza el pago completo del producto, la bomba lógica borre archivos que impidan el buen funcionamiento de la aplicación.

Muchos virus se ejecutan por medio de bombas lógicas en determinadas fechas. Por ejemplo, un empleado que deje de trabajar para la empresa podría activar una bomba lógica con el fin de que a los siete meses después su marcha, un virus infecte todos los ordenadores de la compañía. De esta manera, no levantaría sospechas.

Las bombas lógicas se activan porque se cumplen algunas de las siguientes condiciones:

- ⇒ En una fecha concreta.
- ⇒ En una hora determinada.
- ⇒ Si un contador interno llega a un número concreto.
- ⇒ Se alcanza cierto número de ejecuciones del programa que contiene la bomba lógica.
- ⇒ Si se cumplen otras características establecidas por el atacante.

Por lo tanto, una bomba lógica puede permanecer inactiva durante un largo periodo de tiempo, de manera que nadie nota ningún comportamiento extraño en el sistema hasta que la bomba se activa. En esta característica, radica el poder dañino de las bombas lógicas.

En inglés reciben el nombre de *time bombs*. Pueden realizar diversas acciones, desde mostrar un simple mensaje hasta borrar información importante del disco duro. Debido a que es muy común este tipo de sabotaje por parte de empleados a punto de abandonar la organización, es vital inhabilitarles el acceso a los sistemas para que no puedan acceder desde el momento en el que se les informe de su despido.

3. 3. 1. 5 *Adware*

Los *adware* son aplicaciones que muestran publicidad o la descarga al equipo del usuario cuando éste instala un programa. "*Ad*" es el diminutivo de *advertisement* que en castellano significa anuncio.

Muchos programas de descarga gratuita contienen *adware*. De esta forma, los creadores del programa consiguen un beneficio económico. El usuario, al instalar el programa, no es consciente de la descarga del *adware*. En ocasiones, pueden remplazar la página de inicio del navegador, aparecer ventanas *pop-ups* con publicidad o instalarse aplicaciones no deseadas. Por ejemplo, al instalar un programa, en las opciones que vienen marcadas "por defecto", aceptamos la instalación de una barra de herramientas en nuestro navegador.

Hoy en día, los antivirus incluyen herramientas de detección de *adware*. Sin embargo, toda precaución es poca y los usuarios deben asegurarse que el programa que instalan no contiene *adware* leyendo cuidadosamente el contrato de licencia. Además, se debería instalar alguna herramienta que bloquee las ventanas emergentes y evitar así, las ventanas de *adware*.

3. 3. 1. 6 *Spyware*

El *spyware* o *software* espía envía información personal del usuario a terceros sin que éste tenga conocimiento sobre lo sucedido. Vulneran la privacidad de los usuarios. La información enviada puede ser las páginas web que se visitan o algo más comprometido como contraseñas o números de tarjetas de crédito. Habitualmente las empresas utilizan esa información para enviar publicidad a los usuarios.

Al igual que los *adware*, se pueden instalar al descargar un programa y aceptar las condiciones de uso. Para evitar instalar este *software* malicioso en los equipos de la compañía, lo más adecuado es poner en práctica las medidas comentadas en el apartado de *adware*. Además de los antivirus que los detectan, existen diversos programas *anti-spyware*.

3. 3. 1. 7 Puertas traseras

También son conocidas como *backdoors*. Las puertas traseras permiten a su creador o a personas con conocimiento de su existencia, el acceso a una máquina de forma remota sin que el usuario se percate. Son muy difíciles de detectar. La única forma de cerciorarse que un programa no contiene *backdoors* es revisando el código línea a línea.

Los atacantes, a través de estas puertas traseras, pueden eliminar ficheros, borrar información del disco duro, acceder a datos confidenciales o abrir puertos de comunicaciones permitiendo que un agente externo controle el ordenador de forma remota, entre otras acciones.

Las puertas traseras se crean durante el desarrollo de programas, permitiendo al programador evitar los sistemas de seguridad. Son segmentos de código que agilizan la detección y depuración de fallos en el código, es decir, son como "atajos". Los programadores deben eliminar las puertas traseras antes de finalizar el programa pero, en ocasiones, involuntariamente o de forma intencionada, esto no ocurre y si alguna persona tiene conocimiento de este hecho puede acceder al ordenador suponiendo una amenaza para los usuarios de dicho equipo.

Por ejemplo, si para acceder a una aplicación debemos introducir varias claves de acceso, el programador puede indicar al programa que si se introduce una determinada contraseña como "programador" directamente se acceda a la aplicación, ahorrando tiempo mientras finaliza la aplicación. El programador, cuando obtiene el programa final, debe eliminar esa condición para que nadie acceda al programa a través de esa puerta trasera.

Otro ejemplo, podría ser el acceso a una determinada página web que para su acceso se requiere un nombre de usuario y una contraseña pero que desde otra dirección alternativa es posible acceder sin introducir claves.

Además, una puerta trasera puede estar integrada en un troyano o en cualquier otra aplicación. Se comentó en el apartado de "Troyanos" dos programas que abrían puertas traseras denominados *NetBus* y *BackOrifice*. *SubSeven* también es un troyano que abre una puerta trasera instalando el programa servidor en la máquina anfitriona y realizando acciones maliciosas, como obtener claves, realizar capturas de pantalla o deshabilitar teclas, entre otras.

3. 3. 1. 8 Programa conejo

Un programa conejo o bacteria es un programa que no causa daño de forma directa al sistema pero que se reproduce hasta agotar los recursos del ordenador causando una **denegación del servicio**. Generalmente estos programas se auto-replican de formal exponencial, por lo tanto, de una copia se generan dos, de dos se crean cuatro, de cuatro se generan ocho y así sucesivamente hasta agotar los recursos del procesador, de la memoria, del disco…

3. 3. 1. 9 *Rootkit*

Rootkit es un conjunto de herramientas usadas por agentes externos para acceder sin autorización a un sistema informático. Se esconden a sí mismos al igual que a otros procesos y archivos para encubrir las acciones maliciosas que llevan a cabo los intrusos informáticos. Por ejemplo, si existe alguna puerta trasera, el *rootkit* oculta los puertos abiertos que evidencien la comunicación.

Si el antivirus examina ficheros del sistema o procesos en ejecución, el *rootkit* falsea los datos y el antivirus no puede actuar contra la amenaza. Hoy en día, existen diversas herramientas *anti-rootkits* para detectar y eliminar el *rootkit*.

En el año 2005, vio la luz el caso de la empresa Sony BGM quien utilizaba esta técnica en el *software* anticopia de algunos CDs. El objetivo era salvaguardar sus propios intereses y prevenir el uso ilegal y la copia de sus CDs musicales. Dicho *software*, se instalaba sin el consentimiento del usuario y abría en Windows una brecha de seguridad que facilitaba el acceso a virus, gusanos y troyanos. Los antivirus no detectaban el *rootkit* y si un usuario encontraba y eliminaba los archivos del *software*, la unidad de CD o DVD de su equipo dejaba de funcionar bajo Windows.

3. 3. 1. 10 *Exploit*

Para explicar lo que se entiende por *exploit*, es conveniente detallar lo que se conoce como *bug* en el argot informático. Un *bug* es un error o defecto de un elemento de *software*. El programa realiza acciones no deseadas o no funciona como debería. Cualquier programa instalado en el equipo puede contener errores. Cuanto mayor sea la complejidad de un programa, más posibilidades existen de contener *bugs*. Los *bugs* más delicados son aquellos que afectan a los sistemas operativos.

La única forma de detectar *bugs* en un *software* es realizar múltiples pruebas en busca de fallos. El problema es que es muy complicado probar un programa totalmente ya que se tendrían que realizar millones de pruebas. En ocasiones esos errores en el *software* son introducidos de manera intencionada por los programadores.

Existen programas que no pueden contener *bugs* debido al impacto que podrían causar sobre las personas. Por ejemplo, el sistema operativo del ordenador de un avión o de una máquina del quirófano de un hospital. Se requiere invertir muchas horas en la realización de las pruebas de estos programas.

Los *bugs* suelen corregirse según surgen nuevas versiones de un *software*. Por esta razón, es importante actualizar los programas o instalar parches específicos para resolver los problemas generados por los errores. Si se detecta un *bug* lo adecuado es comunicárselo al fabricante para que lo elimine en sucesivas versiones. La empresa Kentico puso en marcha en el año 2009 el proyecto "*Trees for Bugs*" en el que por cada *bug* que encontrara un usuario en su *software*, la compañía se encargaba de plantar un árbol. Es una buena forma de eliminar errores, de cuidar el medio ambiente y de ahorrarse el sueldo de algunos trabajadores…

Los *exploits* se encargan de aprovechar vulnerabilidades, es decir, aprovechan los *bugs* que contiene el *software*. Suelen ser programas que explotan los errores de un programa para obtener algún tipo de beneficio o privilegio. Los *exploits* pueden violar las medidas de seguridad para acceder a un sistema sin autorización.

Los *exploits 0-day* son aquellos que se crean seguidamente después de descubrir una vulnerabilidad. Son bastante efectivos ya que los fabricantes desconocen todavía esos errores y no existen parches para eliminarlos.

Los usuarios no pueden controlar que los programadores cometan errores en el desarrollo de los programas ni que existan personas que aprovechen esos fallos para realizar acciones maliciosas pero si pueden protegerse. Los usuarios deben realizar copias de seguridad continuamente para prevenir posibles pérdidas de información. Además, deben cerciorarse de tener instalados los últimos parches o actualizaciones del *software*.

3. 3. 1. 11 *Cookie*

Las *cookies* son fragmentos de información acerca de las visitas realizadas a un sitio web que se almacenan en el equipo del usuario. De esta forma, se consiguen una navegación más personalizada ajustando el sitio a las preferencias del usuario y, además, permite medir las preferencias del mercado. Por ejemplo, iGoogle permite personalizar la página según los intereses de la persona, pudiendo visualizar las últimas noticias, juegos, deportes, finanzas, meteorología...

Las *cookies* surgieron para que los servidores web guardaran y recuperaran información acerca de sus visitantes. El inconveniente de las *cookies* es que pueden vulnerar la intimidad si los datos obtenidos pueden asociarse a un individuo. No obstante, las *cookies* no graban datos personales como el nombre o la dirección de correo electrónico, a menos que se facilite esta información.

Es importante recalcar que las *cookies* no tienen acceso al disco duro del usuario. Los usuarios pueden evitarlas cambiando las opciones de la configuración de privacidad del navegador. La persona puede configurar su equipo para que el navegador pregunte si debe aceptar o no cada *cookie*. Además, pueden ser eliminadas por el usuario.

3. 3. 1. 12 *Pharming*

Pharming es una técnica que consiste en manipular las direcciones DNS (*Domain Name System*) a las que accede el usuario, permitiendo a un intruso redirigir un nombre de dominio a otra máquina. La manipulación se realiza por algún código malicioso, generalmente un troyano, que se ha introducido en el ordenador.

En los servidores DNS se almacenan tablas con las direcciones IP de cada nombre de dominio. El *pharming* modifica el sistema de resolución de nombres. El usuario al intentar acceder al sitio web que desea, accede a otra página creada por el atacante para recabar información confidencial del individuo. La persona no sospecha que se encuentra en una página falsa ya que la muestra el mismo aspecto que la original. Esta práctica es muy utilizada en páginas relacionadas con la banca.

El cambio de direcciones DNS puede afectar a todos los usuarios que utilicen el servidor o afectar sólo de forma local, es decir, a cada *host*. Esta última forma, es más peligrosa y se puede llevar a cabo fácilmente en ordenadores que funcionen bajo Windows y utilicen el navegador Internet Explorer, modificando un archivo denominado “hosts”.

Si al intentar acceder a la página web de nuestro banco, el navegador nos redirecciona a otra página sin que tengamos conocimiento de este hecho, es un ejemplo de *pharming*. La página contendrá la misma información que la auténtica por lo que es muy difícil darse cuenta del engaño. De esta forma, se puede facilitar los datos bancarios al atacante.

Para detectar esta práctica, es apropiado contar con un *software* antivirus que combine sistemas de detección proactivos y reactivos. Los sistemas de protección proactivos son capaces de adelantarse a las amenazas y bloquearlas. Es importante actualizar el explorador y el correo electrónico con los últimos parches de seguridad que existan. Además, se ha de contar con un cortafuegos bien configurado evitará que agentes externos accedan al ordenador a través de un puerto de comunicaciones desprotegido.

3. 3. 1. 13 *Spam*

Un *spam* o correo basura es un mensaje publicitario enviado al correo electrónico de un gran número de usuarios sin que éstos lo hubiesen solicitado. Sobrecargan los servidores de correo y los usuarios tienen que invertir tiempo en eliminarlos.

3. 3. 2 *Crimeware*

Cuando el *software* malicioso produce pérdidas económicas al usuario del equipo atacado, también se denomina como *software* criminal o *crimeware*. Por ejemplo, forman parte de esta clasificación:

- Técnica del salami
- *Carding*
- *Scam*

3. 3. 2. 1 *Scam*

La palabra s*cam* significa estafa en castellano. Un *scam* es una técnica que cosiste en el envío de correos electrónicos que contienen una propuesta con el fin de estafar económicamente al usuario. Pueden ofrecer grandes sumas de dinero o un trabajo muy bien remunerado para captar la atención de la persona. También se le denomina *scam* a páginas web que ofrecen algún producto o servicio falso con el fin de estafar al usuario.

Cuando recibimos un *email* ofreciéndonos una gran suma de dinero por realizar un cómodo trabajo, estamos seguramente, ante un ejemplo de *scam*. Los estafadores solicitan el número de cuenta bancaria de varios usuarios con alguna excusa (*phishing*). Después retiran grandes sumas de dinero de esos usuarios a través de los intermediarios (las personas que han aceptado el fabuloso trabajo ofrecido anteriormente). El trabajo de los "empleados" consiste en reenviar ese dinero a los estafadores, ganando así, una comisión. Consciente o inconscientemente, los "empleados" son cómplices de un delito de robo y blanqueo de dinero. En este caso, son víctimas las personas robadas y los "empleados" que no conocían la estafa en la que participaban.

3. 3. 2. 2 *Carding*

El *carding* consiste en la utilización ilegal de tarjetas de crédito ajenas. Se utiliza un número de tarjeta perteneciente a otra persona para realizar compras a través de Internet. La persona que comete el fraude puede conseguir el número de la tarjeta a través de:

- **Recogida de información residual**: consiste en aprovechar la información depositada en la papelera que no ha sido destruida. El atacante se beneficia del descuido o ignorancia de los empleados que no vacían las papeleras al depositar documentos valiosos. De esta manera, se obtiene acceso a información privilegiada sin autorización para ello. En algunos textos, denominan a esta amenaza lógica *scavenging*, *trashing* o basureo.

  No es una práctica muy utilizada pero se debe tener especial cuidado con esta técnica debido a que se puede recabar de una manera muy sencilla información tan relevante como contraseñas de usuarios, datos bancarios, teléfonos o información confidencial de los trabajadores de la compañía.

- ***Keyloggers***: programas que almacenan las teclas pulsadas por el usuario para capturar el número de las tarjetas de crédito y las contraseñas, entre otra información.

- **Troyanos**: ya explicado en el apartado de *malware*.

En resolución, los bancos han implantado más medidas de seguridad para identificar y autenticar al usuario y aumentar así, la confianza de los usuarios en la utilización del comercio electrónico.

3. 3. 2. 3 Técnica del salami

La técnica del salami consiste en desviar de forma fraudulenta pequeñas cantidades de bienes (habitualmente dinero) de diversas fuentes que posean una gran cuantía de ellos, de manera que sea casi imperceptible el robo de una pequeña cantidad. Al igual que cortar una fina rodaja de una barra de salami, en ésta no se percibe un cambio significativo de tamaño. De este hecho recibe el nombre de técnica del salami. Se utiliza generalmente en sectores relacionados con la banca.

Por ejemplo, si una persona posee en su cuenta bancaria 1330,27 euros y le roban 500 euros el individuo se dará cuenta inmediatamente de este suceso. En cambio, si el autor del robo extrae 5 céntimos de esa cuenta, el usuario de la cuenta no notará la diferencia ya que es una cantidad demasiado pequeña para que se percate del robo y, si lo descubre, es posible que no reclame una cantidad tan ínfima y lo deje pasar por no perder tiempo en saber dónde están sus 5 céntimos ni reclamarlos. Si el ladrón sustrae 5 céntimos en 5.000.000 de cuentas bancarias recaudará un total 250.000 euros.

3. 3. 3 Ingeniería social

La ingeniería social consiste en la manipulación de las personas para que de manera voluntaria, lleven a cabo actos que de otro modo no realizarían. Es una técnica muy sencilla y desafortunadamente, muy efectiva.

Por ejemplo, se utiliza la ingeniería social cuando se descarga un programa de Internet pensado que es un antivirus para el ordenador y, de esta forma, estar a salvo de posibles amenazas. Al ejecutar el programa la computadora es infectada por un troyano. Si al descargar el *software* para su equipo, en lugar de llamarse “Antivirus X” se denominara “Troyano”, nadie lo descargaría.

Otro ejemplo, podría ser que un atacante envíe un correo electrónico diciendo que ha habido un problema en el sistema y que debe cambiar la contraseña por otra que él le facilita. También podría hacerse pasar por su banco y pedirle su número de tarjeta y su contraseña para empezar a disfrutar del servicio de banca electrónica.

Nunca se debe facilitar contraseñas y ni datos confidenciales por teléfono, correo electrónico o cualquier otro medio de comunicación que no permita identificar al receptor de dicha información. Tampoco debemos ejecutar programas de los que se desconozca el origen.

Los atacantes se aprovechan de los usuarios confiados y de su falta de cultura en medidas de seguridad. El *phishing* es un ejemplo de técnica que utiliza la ingeniería social y el *scam* ya comentado anteriormente.

3. 3. 3. 1 *Phishing*

El *phishing* es una técnica que consiste en la suplantación de identidad de una persona o entidad para obtener datos confidenciales de forma ilícita a través de correos electrónicos. Es considerado como un ***malware***, además de cómo una técnica de ingeniería social.

Esta práctica es muy común en el sector bancario. Los estafadores imitan la imagen de la entidad bancaria y solicitan al usuario que confirme determinados datos personales como el número de tarjeta de crédito con alguna excusa.

La única manera de no caer en este tipo de fraude es la precaución. No se debe facilitar datos personales por correo electrónico ya que nuestro banco no nos pedirá información confidencial por esta vía. Hay que desconfiar de los mensajes que piden cualquier tipo de información personal por problemas técnicos, para recibir un premio o con cualquier otro pretexto.

Es importante destacar que estos mensajes que se reciben suelen estar poco personificados ya que se envían a un gran número de usuarios con el fin de engañar a la máxima cantidad de personas posible.

Asimismo, debemos fijarnos muy bien en los enlaces que contienen los correos electrónicos. Podría suceder que accediéramos a una imitación de la web que deseamos visitar. Por ejemplo, es posible que queramos acceder a la página de nuestro banco y al visitar el enlace que contiene el *email* no nos demos cuenta que la dirección de la página web es casi idéntica a la que queríamos acceder pero con algún carácter de más o de menos. De esta forma, la página nos resultará conocida y podríamos facilitar datos confidenciales a terceros.

3. 3. 4 Ataque de denegación de servicio

Un ataque de denegación de servicio o ataque **DoS** (*Denial of Service*) es un ataque que imposibilita el acceso a un recurso o servicio por parte de un usuario legítimo.

Los ataques de denegación de servicio pueden materializarse de distintas maneras formas:

- Consumir los recursos del ordenador como espacio de disco, ancho de banda, o tiempo del procesador.
- Impedir o alterar información de configuración como información de rutas de enrutamiento.
- Alterar o destruir componentes de una red.

De esta forma, se impide el uso del servicio por parte de los usuarios. Estas amenazas atentan principalmente contra la disponibilidad. En el caso de que para provocar la denegación de servicio se recurriera a la suplantación de identidad también se atentaría contra la autenticación de la información.

Es una práctica muy utilizada por los *crackers* para provocar la caída de un servidor. El servidor recibe demasiadas peticiones, provocando que se sature y no pueda dar servicio a los usuarios legítimos.

Algunos ejemplos de ataques DoS son:

- **SYN *Flood***: *Flood* significa inundación en castellano. Se produce una denegación de servicio debido a que el sistema recibe más peticiones de conexión de las que puede atender.
- ***Smurf***: consiste en enviar a una dirección de *broadcast* una petición de ICMP (protocolo de control y notificación de errores). Se falsifica la dirección de origen (con una técnica denominada *spoofing)* que será la víctima del ataque. Cada *host* mandará una respuesta a la dirección IP de la víctima, provocando así, una denegación de servicio.
- **Ping de la muerte o *ping of death***: Un atacante podría modificar el tamaño del paquete que envía a otra máquina superando el máximo autorizado (65535 Bytes) para producir un desbordamiento de memoria en el *host* atacado causando una denegación de servicio.

Actualmente, las máquinas no son vulnerables a este tipo de de ataque.

- ***Email bombing***: consiste en enviar gran cantidad de correos electrónicos a los usuarios para saturar los servidores de correo.

Un tipo de ataque de denegación de servicio es **DDoS** (*Distributed Denial of Service*) o denegación de servicio distribuida. Se instalan varios agentes remotos en diversos equipos denominados *zombies*, controlados por un tercero. Los ordenadores *zombies* son computadoras que han sido infectadas por algún tipo de código malicioso (por ejemplo, un troyano) que permite a una tercera persona controlar la máquina remotamente. El atacante coordina los equipos para que el ataque sea más efectivo, consiguiendo mayor saturación del recurso. Estos ordenadores solicitan un servicio de manera simultánea, colapsándolo.

3. 3. 5 Ataque de modificación o daño

Un intruso no autorizado accede al contenido de la información y la altera de forma que los datos que recibe el destinatario difieren de los originales. Este tipo de ataques atentan principalmente, a la integridad de la información.

A continuación, se explican algunos ejemplos de este tipo de ataques como son: el *data diddling o tampering*, los a*pplets* hostiles, ataques *ActiveX* y el borrado de huellas.

3. 3. 5. 1 *Data diddling*

Esta práctica consiste en la alteración no consentida de los de datos, (modificar datos, borrarlos o introducir datos falsos) o la instalación de *software* en el sistema. El administrador podría necesitar dar de baja el sistema durante unas horas o días para examinar la información e intentar recuperar los datos alterados. También recibe el nombre de ***tampering***.

Algunos ejemplos de esta técnica son: modificar las calificaciones de un alumno en el sistema de la universidad o modificar el nombre un *software* malicioso como algún conocido programa que las personas se descarguen, adhiriéndole un virus. Dentro de esta categoría se incluyen los virus, gusanos, troyanos y bombas lógicas y otras amenazas similares.

3. 3. 5. 2 *Applets* hostiles

Un *applet* es un componente de *software*, generalmente de pequeño tamaño, escrito en un lenguaje de programación como Java, que se ejecuta bajo el control de una aplicación que lo contiene (por ejemplo, un navegador web).

Java es un lenguaje de programación bastante seguro, pero también muestra algunos puntos débiles. Los *applets* de Java pueden ejecutarse en cualquier plataforma y en cualquier sistema operativo. Esto es una característica del lenguaje bastante interesante desde el punto de vista de Internet.

El problema reside en que si desde cualquier página web podemos recibir un *applet* que se ejecute en nuestro ordenador, esto abre puertas a posibles ataques a seguridad del sistema como: introducir virus, conseguir información importante de nuestra computadora o que el cortafuegos deje de realizar su función.

Además de ser un problema que perjudica al lenguaje Java, también afecta a cualquier tipo de código ejecutable que pueda descargarse y ejecutarse en nuestro equipo, como páginas que utilizan JavaScript o VBScript.

Para evitar amenazas que afecten a la seguridad de los equipos de la empresa, se ha de evitar instalar *applets* de origen desconocido. Además, no se debe ejecutar el navegador web desde un equipo que almacene información crítica, como un servidor.

3. 3. 5. 3 Ataques *ActiveX*

ActiveX es un conjunto de tecnologías desarrolladas por Microsoft para incluir dinamismo en el entorno web. Un control *ActiveX* es un fragmento de código ejecutable que al descargarlo el usuario está permitiendo que el control se ejecute sin restricciones.

Muchos empleados aceptan los controles sin conocer su origen y, en ocasiones, pueden suponer una amenaza para los sistemas. Para evitar posibles daños, algunas compañías no permiten la instalación de controles *ActiveX*. Otras, en cambio, permiten la instalación pero tratan de detectar cualquier *software* malicioso que se instale.

ActiveX recurre a certificados y firmas digitales para evitar controles dañinos. Las autoridades certificadoras remiten certificados que se asocian a los controles activos y a una firma digital del programador.

3. 3. 5. 4 Borrado de huellas

En los archivos *logs* se almacena información sobre los cambios que se realizan sobre el sistema. El atacante cuando se adentra en el sistema, pretende evitar que se detecte su ingreso para pasar desapercibido y que el administrador no tome medidas de seguridad para evitar que se materialice el ataque nuevamente.

Por lo tanto, el borrado de huellas consiste en modificar los *logs* del sistema en los que queda reflejado las distintas acciones realizadas para evitar que se detecte su acceso ilícito.

3. 3. 6 Ataque de suplantación

Los ataques de suplantación (fabricación o impostura) pretenden suplantar a un usuario o una máquina por medio de distintas técnicas para conseguir el acceso a la información. Este tipo de ataques atentan contra la autenticación principalmente.

Habitualmente se lleva a cabo obteniendo la contraseña y el identificador de un usuario por medio de distintos mecanismos. Otras veces el atacante pretende hacerse pasar por un usuario o entidad legítima para hacer creer a su víctima que es la persona que dice ser. Este último caso, es lo que realiza la técnica ***phishing*** ya explicada anteriormente, a través de correos electrónicos.

3. 3. 6. 1 *Spoofing*

Se suplanta la identidad de una máquina o usuario legítimo para realizar acciones sobre un sistema. Por ejemplo, el intruso puede conseguir el nombre y contraseña del usuario autorizado y enviar falsos correos electrónicos en nombre de la víctima.

Cuando el ataque de falseamiento se realiza una dirección de IP se conoce como **IP *spoofing***. El atacante consigue que el receptor de los mensajes crea que recibe tramas del emisor legítimo. El intruso simula la identidad de otra máquina para conseguir acceso a recursos de un sistema con el nombre o la dirección IP del equipo suplantado.

Un ataque IP *spoofing* puede utilizarse para producir ataques de denegación de servicio. Si se suplanta la dirección IP del emisor y se envían mensajes a distintas máquinas, éstas enviarán sus respuestas a la dirección IP de la víctima, provocando una denegación de servicio (*smurf*).

Alberto Luis Corrales y otros autores proponen en su libro "*Diseño e implantación de arquitecturas informáticas seguras: una aproximación práctica*" como posible solución al IP *spoofing*: evitar las relaciones de confianza basadas en las direcciones IP, estableciendo relaciones fundamentadas en claves criptográficas o en autenticación utilizando Kerberos.

Existen más ataques de suplantación de identidad como DNS *spoofing* (resolver una dirección IP falsa a un cierto nombre DNS o viceversa), *Mail spoofing* (se suplanta de una dirección de correo electrónico) o Web *spoofing* (se suplanta una página web), todas con el objetivo común de falsear la identidad de un usuario o máquina y realizar acciones maliciosas.

3. 3. 6. 2 *Hijacking*

Hijacking (o secuestro en castellano) hace referencia a cualquier acción ilícita que lleve a cabo un atacante cuyo fin sea apropiarse de algo, generalmente de información.

En materia informática se pueden destacar el secuestro de sesiones (*session hijacking*), de páginas web (*page hijacking*), de navegadores (*browser hijacking*), de la página de inicio de los navegadores (*home page browser hijacking*) o dominios (*domain hijacking*), entre otros.

3. 3. 7 Ataque de monitorización

Los ataques de monitorización o intercepción son aquellos en los que una tercera parte no autorizada, busca vulnerabilidades en el sistema para acceder al contenido de la información con el objetivo de apropiarse de ésta pudiendo hacer uso de ella con fines ilícitos. Son ataques que atentan contra la confidencialidad de la información.

En este tipo de ataques se incluyen:

- **Señuelos** o *decoy*: programas que imitan la interface que otro original para solicitar el nombre de usuarfuo y la contraseña y guardar esta información para acceder al sistema.
- ***Keyloggers***: programas que almacenan las teclas pulsadas por el usuario para conocer contraseñas o cualquier información confidencial y realizar acciones maliciosas.
- ***Scanning*** o búsqueda: Se escanean los puertos abiertos para explotarlos posteriormente.

3. 3. 7. 1 *Sniffing*

El *sniffing* consiste en capturar cualquier paquete que circulan por la red. Se puede realizar *sniffing* por *software* o por *hardware*. En este último caso, se conecta un dispositivo a un cable de red para capturar los paquetes que viajen a través del cable (esta práctica recibe el nombre de *wiretapping*).

Generalmente el *sniffing* se realiza por *software*. Un programa captura la información de la red almacenándola, habitualmente, en un fichero al que accede el atacante. Las tramas que circulan por delante de la máquina en la que se encuentra instalado el *sniffer* son captadas aunque la información no vaya dirigida a dicha máquina.

Un símil a mencionar serían los cuerpos de seguridad interceptando llamadas entre delincuentes para obtener información que les pueda ser útil. El *sniffer* realiza la misma acción que los agentes pero como fines menos honestos. Se queda "escuchando" para captar contraseñas, números de tarjeta de crédito, direcciones de correo electrónico o cualquier otra información ya que, en ocasiones, estos datos no viajan cifrados.

Es muy complicado detectar esta técnica. Lo más conveniente es cifrar toda la información sensible que circule por la red. Protocolos como "ssh" o "https" cifran la información. Esto no impide que no se capten los paquetes pero sí evita que sean legibles para el atacante.

3. 3. 8 Redes sociales

Las redes sociales han surgido en los últimos años para revolucionar la manera de comunicarnos vía Internet. Estas redes, nos permiten mostrar y compartir fotos, videos, comentarios, etc. Sin embargo, en ocasiones, suponen una amenaza en nuestra seguridad tanto física como lógica.

A través de los mensajes publicados, los vídeos y las fotos, es fácil que los demás usuarios conozcan dónde nos encontramos, quiénes son nuestros amigos y familia y qué hacemos en cada momento. Estas acciones nos colocan en el punto de mira de un atacante.

Por ejemplo, un usuario de una red social como Facebook o Tuenti podría publicar en su perfil que está de vacaciones con toda su familia en otra ciudad y qué día volverá. Si alguien quisiera atracar su casa, le habría facilitado mucho la labor... Además, si el usuario tiene publicadas fotos de su casa, su coche o cualquiera de sus bienes, estaría en conocimiento de muchos detalles acerca de su vida.

El perfil de una red social puede configurarse para que solamente determinados usuarios accedan a su perfil, aumentando así su privacidad. Pero esto no es suficiente para estar libres de peligro.

Relativo a la seguridad lógica, un intruso podría crearse un perfil con el nombre y apellidos de un tercero conocido por la víctima. De esta manera, la víctima aceptaría a su supuesto amigo para que ambos pudieran comunicarse a través de la red social. El intruso, haciendo uso de la **ingeniería social**, podría solicitarle información personal para hacer uso ilícito de ella.

Otra amenaza de la seguridad lógica radica en que estas redes sociales se han convertido en un medio para propagar ***malware***. En varias redes como Facebook, es posible el intercambio de pequeñas aplicaciones realizadas por terceros que no han sido desarrolladas por los informáticos de la propia red. Algunas de estas aplicaciones con aspecto inofensivo contienen código malicioso. Las aplicaciones pueden ser recomendadas por sus amigos o familiares, lo que dificulta que estos usuarios desconfíen. Estas redes están envueltas en un halo de confianza y hacen que los usuarios no se conciencien de la falta de seguridad.

Una solución podría ser contratar programadores para que revisaran el código de las aplicaciones externas. El coste que supondría para las redes sociales es inviable. Se prevé que este tipo de ataques aumenten a medida que evolucionen las redes sociales.

3. 4 Métodos de protección

La primera pregunta que debemos plantearnos cuando la entidad sufre un ataque es ¿**cómo**?, después ya se preguntará por el quién, dónde o cuando. La empresa debe implementar controles para evitar sufrir incidentes. Si la compañía sufre un ataque puede ocurrir lo siguiente:

- **El ataque falla**: deben estudiarse estos ataques para comprobar que los controles que se han implementado funcionan como deben y que el ataque no se haya materializado por un golpe de suerte, pudiendo tener éxito en el futuro.
- **El ataque se ha materializado parcialmente**: el intruso ha podido burlar algunos mecanismos de seguridad pero ha sido frenado por otros. La empresa debe poner los medios necesarios para evitar que se puedan eludir nuevamente los controles.
- **El ataque ha tenido éxito**: la compañía debe disponer de herramientas que le avisen que ha sufrido un incidente. Además, debe poner en marcha un plan de recuperación.

Para proteger los ordenadores de posibles ataques, la compañía ha de implementar todas las medidas de seguridad que estén a su alcance y mostrar una actitud lo más alerta posible en cuanto a seguridad se refiere. Cualquier acto o acción que no esté explícitamente autorizada, no debería poder llevarse a cabo.

Entre las medidas a poner en práctica, es vital el uso de un buen antivirus actualizado, contar con un firewall bien configurado, realizar copias de seguridad con frecuencia, hacer uso de técnicas de cifrado y auditorías, entre otras. A continuación, se explican con más detalles los antivirus, cortafuegos y la realización de *backups*.

3. 4. 1 Antivirus

Los antivirus son herramientas encargadas de prevenir la infección de los ordenadores, además de detectar y eliminar virus y otras amenazas lógicas de los equipos informáticos.

Desafortunadamente los virus suelen adelantarse a los antivirus. Cada día, se programan nuevos códigos maliciosos que los antivirus tardan en reconocer. Por este motivo, no son completamente fiables.

Los antivirus tienen tres funciones importantes que son:

- **Vacuna** o **Motor del antivirus**: Programa que actúa como un filtro para analizar en tiempo real si existe algún archivo o programa que al ejecutarse infecta el ordenador.
- **Detector**: Programa que se encarga de escanear los archivos, directorios o unidades que seleccionemos para detectar códigos maliciosos, capturarlos y detenerlos.
- **Desinfectador**: Programa que una vez que encuentra el virus lo elimina y repara sus efectos en el sistema. En ocasiones, el antivirus no puede eliminar el virus y lo mantiene en cuarentena hasta encontrar la cura.

Los antivirus pueden clasificarse en:

- Antivirus basados en **firmas**: el antivirus contiene una gigantesca base de datos con las huellas o firmas de todos los virus que se conocen. Por este motivo es importante actualizar con frecuencia el antivirus, siendo lo ideal diariamente. En ocasiones, el antivirus no reconoce un nuevo virus debido a que todavía no está incluido en la base de datos.
- Antivirus basados en **detección heurística**: posee un comportamiento basado en reglas. Compara el contenido de los archivos con unos criterios preestablecidos en busca de posible código maliciosos.

3. 4. 2 Cortafuegos

Según escribe Carmen España en su libro "*Servicios avanzados de telecomunicación*", un cortafuegos es "*un sistema de seguridad desarrollado para ubicarse entre una red pública, generalmente Internet, y una red interna perteneciente a una organización, o bien entre diferentes secciones de una red interna*."

Un cortafuegos o ***firewall*** funciona de filtro entre redes facilitando las comunicaciones autorizadas y evitando los accesos ilícitos. Entre los objetivos de un cortafuegos se encuentra: evitar que usuarios de Internet accedan sin autorización a redes privadas conectadas a Internet y, permitir sólo el tráfico autorizado a través de políticas de seguridad preestablecidas.

El *firewall* debe colocarse entre las dos redes de forma que recoja todo el tráfico que circule entre ambas redes. Una red envía paquetes a la otra, y viceversa. Los paquetes son mensajes que contienen datos y cuentan, además, con una cabecera.

La cabecera contienen información como:

- Dirección IP de origen y dirección IP de destino: las direcciones IP son un conjunto de números que identifican unívocamente a cada máquina dentro de la red. La direcciones IP pueden ser fijas o dinámicas (cambian cada vez que te conectas).
- Puerto de origen y puerto de destino: los puertos son canales de comunicación de los ordenadores en la red. Por ejemplo, el puerto 80 esta asignado para el servicio web.
- Tipo de mensaje: De los tipos de mensajes cabe destacar los mensajes TCP, UDP e ICMP. Los dos primeros tipos son mensajes de datos y los ICMP son mensajes de control.

Por otro lado, los cortafuegos pueden ser:

- ***Firewalls* de *software***. Se instala un programa en la máquina que actúa de cortafuegos. También reciben el nombre de *firewall* personal. No tienen un precio demasiado elevado.
- ***Firewalls* de *hardware***. Son más costosos que los cortafuegos de *software* y más complicados de utilizar. Estos cortafuegos normalmente están instalados en los *routers* que utilizamos son más adecuados para organización que cuentan con varios equipos conectados.

Los cortafuegos constan de varios componentes:

- **Filtrado de paquetes**: pretende evitar los accesos no autorizados implementando diferentes políticas de seguridad. El usuario configura el cortafuegos según sus necesidades, es decir, el individuo marca el grado de permisividad que desea en el tráfico de paquetes a través de unas normas preestablecidas.

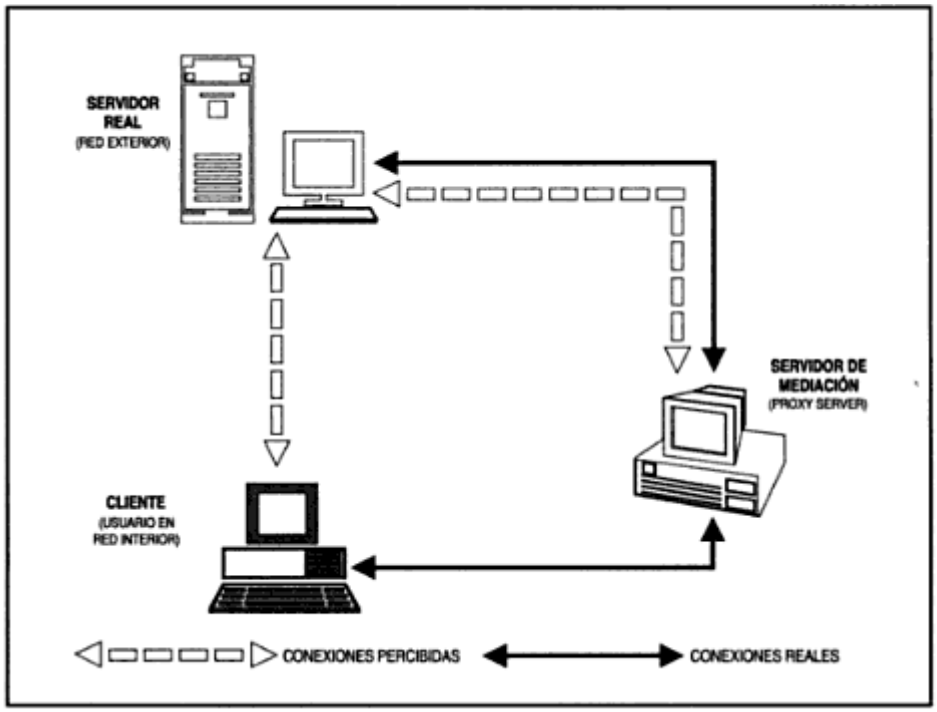
  La política de un cortafuegos puede ser permisiva o restrictiva. Si es una **política permisiva** (*allow everything*), el *firewall* permite todo el tráfico excepto el que está denegado de antemano. En el caso que la política sea **restrictiva** (*deny everything*), deniega todo el tráfico excepto el que está previamente autorizado.

  Generalmente el filtrado consiste en analiza la cabecera de los paquetes y en función de la política establecida previamente, la trama es permitida o denegada.

- ***Proxy* de aplicación**: además del filtrado de paquetes, los cortafuegos suelen utilizar estas aplicaciones *software* que actúan de intermediarias entre los usuarios de la red interna y los servidores de Internet. El programa dialoga con servidores exteriores en representación de los clientes de la red interna. La máquina donde se ejecutan estas aplicaciones se denomina pasarela de aplicación.

  Como se muestra en la siguiente figura, el cliente dialoga con el servidor real a través del servidor de mediación (*Proxy Server*).

Figura 3.2 Uso de *Proxy Server*

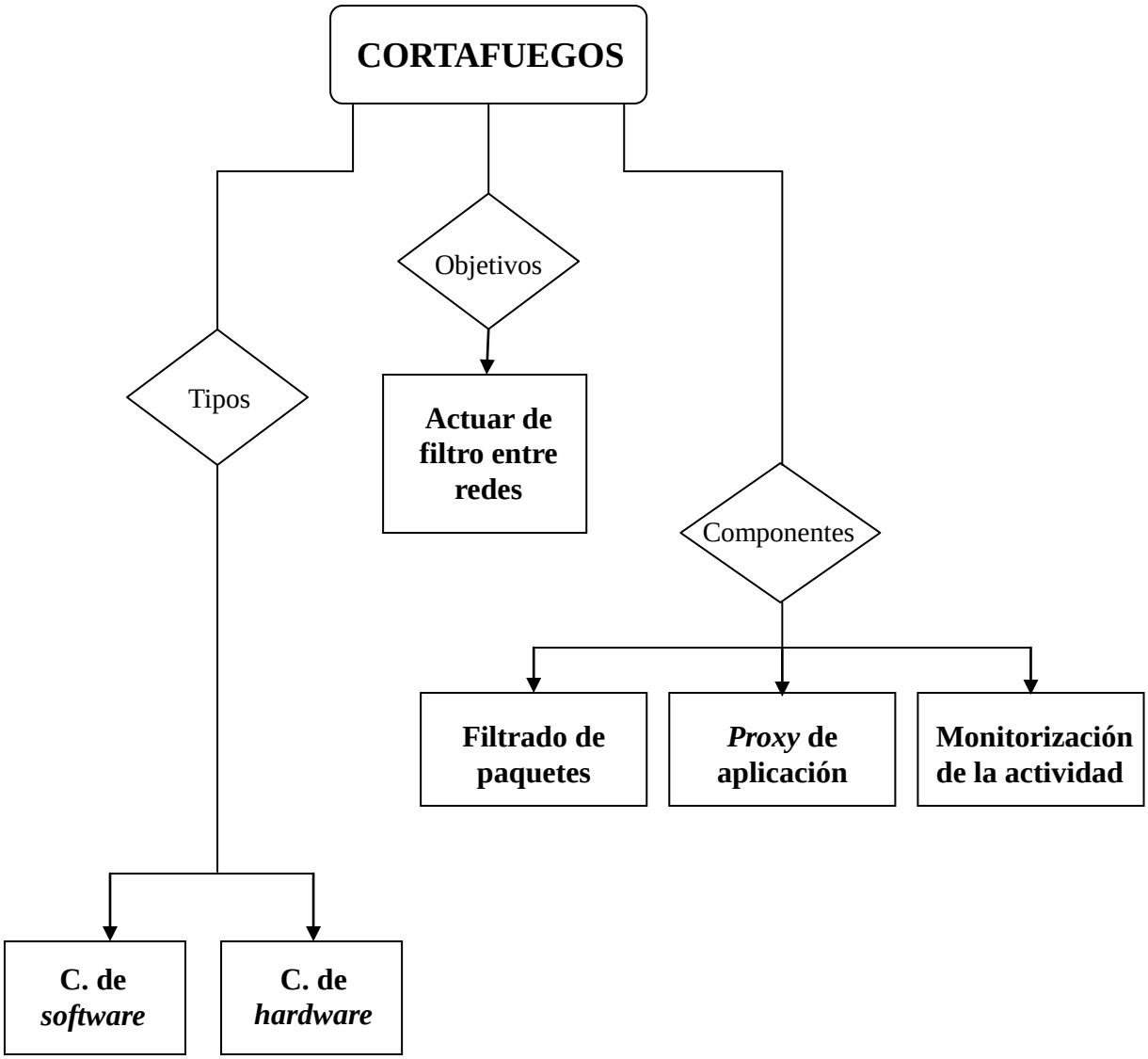


Fuente: "*Reingeniería y seguridad en el ciberespacio*". J.A. Calle Guglieri. Editorial Díaz de Santos, S.A.

- **Monitorización de la actividad**: facilita información sobre los intentos de accesos ilícitos, registrando el origen, horario, tipo y otras características del ataque.

Si se instala un cortafuegos, lograremos que sea más difícil que nuestro sistema sufra intromisiones no deseadas. Aunque los *firewalls* son mecanismos importantes en la seguridad lógica, éstos no protegen completamente al sistema de posibles ataques. Por ejemplo, los cortafuegos no previenen ataques internos, como podría ser que un empleado copie información confidencial del sistema o instale un virus en los ordenadores de la empresa. Tampoco puede proteger de aquellos ataques que no se produzcan a través del *firewall*.

Figura 3.3 Cortafuegos



3. 4. 3 Copia de seguridad

En este documento, ya se ha comentado la importancia de la información para las empresas. Las entidades dependen en gran medida de sistemas computarizados para organizar la información. Si pierden dicha información por un desastre o un fallo puede repercutir en grandes pérdidas económicas, de imagen, etc.

Las copias de seguridad se utilizan con el fin de recuperar la información del sistema en el caso de que se produzca la pérdida de la misma. La información se almacena en dispositivos de almacenamiento que se depositan en un lugar seguro. De esta manera, se consigue restaurar el sistema en el caso de que se produzca un fallo.

Los fallos en el sistema pueden ser:

- Físicos: se originan fallos en el *hardware*.
- De diseño: se producen fallos en los programas.
- De operación: causados por la intervención humana.
- De entorno: producidos por desastres naturales o del entorno.

Realizar copias de seguridad o *backups* es vital para la continuidad del negocio. La fiabilidad de los datos almacenados en las copias de seguridad dependerá de la frecuencia con la que se realicen tales copias y de la frecuencia con la que actualice la información de la compañía. La periodicidad con la que se realicen *backups* dependerá de la empresa, del grado de criticidad de la información y del nivel de actualización de ésta. Por ejemplo, un banco necesita realizar copias de seguridad constantemente ya que a cada momento, se están actualizando datos en las cuentas bancarias de los clientes.

Existen varios tipos de *backups*:

- **Copias de seguridad integrales o completas**: se realizan copias del fichero completo sin tener en cuenta que la información ya hubiera sido copiada. Generalmente se realizan semanalmente.
- **Copias de seguridad incrementales**: copia los archivos que tienen activado el atributo de modificado, es decir, sólo se copia la información actualizada. Cuando se realiza la copia de seguridad el atributo de modificado se desactiva. Se realiza una copia completa del fichero únicamente la primera vez que se copia. Ahorra espacio pero para recuperar un fichero es necesario recurrir a la última copia completa y a todas las copias incrementales realizadas hasta el momento.

- **Copias de seguridad diferencial**: es muy similar a los *backups* incrementales. La diferencia reside en que el atributo de modificado no se desactiva hasta que no se realiza un *backup* completo o incremental. Para recupera un fichero se utiliza la última copia completa y la última diferencial. Por este motivo, la recuperación de archivos es más rápida que con copias incrementales aunque necesitan más dispositivos de almacenamiento.

A continuación, se muestra una tabla de comparación de copias de seguridad según tiempo y espacio que necesitan.

Figura 3.4 Comparación de tipos de *backups*

Tipo de backup	Completo	Incremental	Diferencial
Dispositivos a usar	Mayor número	Menor número	Menor que la completa
Velocidad de backup	Menor	Mayor	Mayor que la completa
Velocidad de recuperación	Mayor	Menor	Mayor que la incremental

Fuente: ""*Informática para las Oposiciones a la Comunidad Autónoma de las Illes Balears*" (2002). Editorial MAD-Eduforma.

Es posible combinar copias completas e incrementales o *backups* completos y diferenciales pero nunca combinar copias de seguridad incrementales y diferenciales ya que se podrían perder información desde el último *backup* completo.

En la siguiente tabla, se muestra la relación entre espacio y tiempo según la combinación de tipos de *backups*.

Figura 3.5 Comparación de *backups* combinados

Tipo de backup	Completo e incremental	Completo y diferencial
Dispositivos a usar	Menor número	Mayor número
Velocidad de backup	Mayor	Menor
Velocidad de recuperación	Menor	Mayor

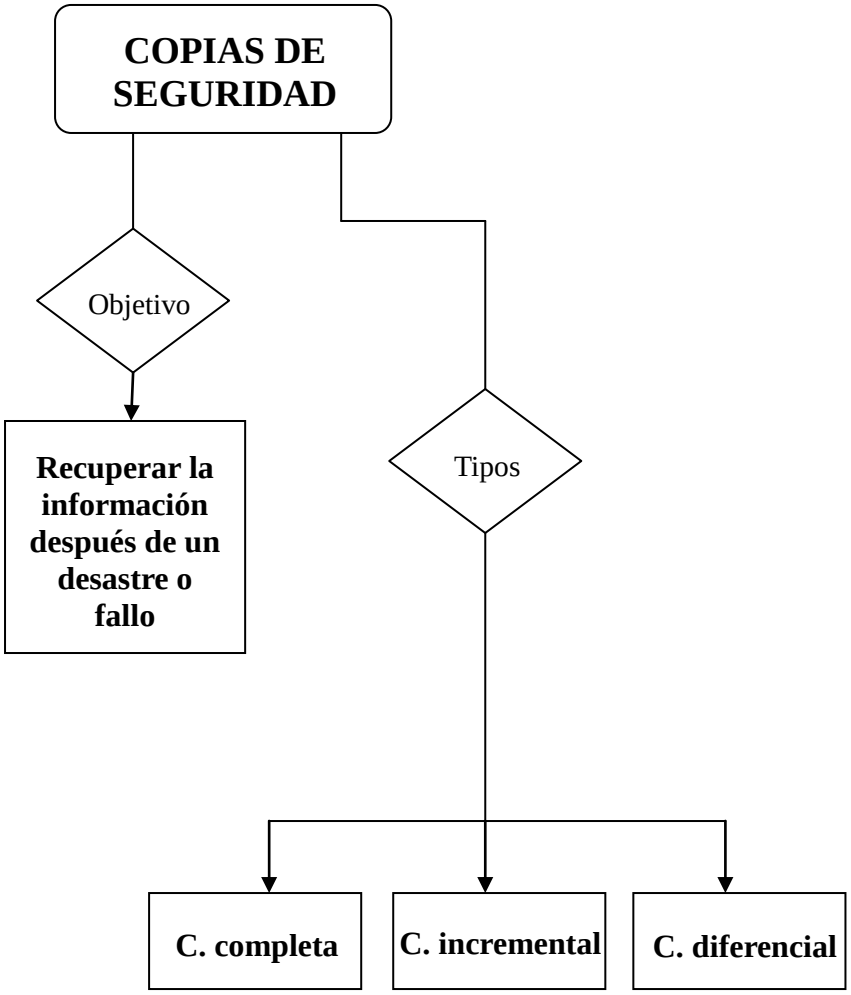
Fuente: "*Informática para las Oposiciones a la Comunidad Autónoma de las Illes Balears*" (2002). Editorial MAD-Eduforma.

Los dispositivos que se utilizan para llevar a cabo los *backups* son diversos, desde cintas magnéticas, CDs, DVDs, *pendrives*… hasta centros de respaldo remotos propios o vía Internet. Las copias de seguridad se suelen realizar de forma automática cuando se trata de grandes sistemas, utilizando aplicaciones *software* específicas para ese fin.

Los *backups* deben almacenarse en lugares seguros y lo más alejados posibles de la información respaldada. De nada sirve tener copias de seguridad actualizadas en un armario de las instalaciones donde se encuentra la información si un incendio puede destruir el edificio y acabar con ellas.

Es importante conocer el tiempo con el que se dispone para realizar el *backup*. Mientras se efectúa la copia, es oportuno no realizar modificaciones sobre los ficheros que se estén respaldando. Por este motivo, es necesario planificar el tiempo del que se dispone para realizar las copias que dependerá, en gran medida, de la cantidad de información que haya que respaldar, el tipo de copia y el dispositivo utilizado, y así, evitar que afecte al funcionamiento normal del sistema.

Figura 3.6 Copias de seguridad



IV. AUDITORÍA

4. 1 Introducción

Una auditoría es un examen sistemático de la situación de una empresa de manera objetiva con el fin de verificar el grado de correspondencia entre la realidad con lo preestablecido y la adecuación de los resultados obtenidos por la compañía a los objetivos perseguidos por la misma.

En una auditoría se realiza una evaluación de las actividades que se llevan a cabo en la entidad auditada para detectar vulnerabilidades e identificar amenazas, emitiendo una serie de recomendaciones para paliar las debilidades. Además, los auditores comprueban que las actividades se ejecutan de forma adecuada.

Es posible distinguir tres fases en una auditoría:

- ⇒ La "**toma de contacto**": se realizan las actividades referentes a la preparación de la auditoría. En esta fase se recopila toda la información necesaria para llevar a cabo la auditoría, los objetivos, el alcance de la auditoría, los recursos necesarios y el plan de trabajo.
- ⇒ **Desarrollo de la auditoría**: utilizando herramientas y técnicas, se obtienen evidencias y se identifica qué se debe mejorar en la organización.
- ⇒ Se elabora el **informe** final: que contendrá los puntos débiles y los fuertes, las posibles mejoras y qué conclusiones se han obtenido.

Es importante no confundir los términos de auditoría y consultoría. La auditoría señala si "las cosas" se están haciendo bien o no, y ofrece las recomendaciones oportunas sobre qué habría que hacer para mejorar en la compañía. En cambio, la consultoría indica cómo llevar a cabo esas mejoras. En general, los consultores no pueden ser auditores de algo en lo que han participado, ni viceversa.

La **auditoría informática** se puede definir como el "*proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, cumple eficazmente los fines de la organización, y hace uso eficiente de los recursos.*"

Las auditorías informáticas mejoran la seguridad, rentabilidad, eficacia y eficiencia de la compañía. Las tareas que se realizan en una auditoría informática pueden agruparse en cuatro categorías:

- Revisión de los sistemas en desarrollo: se evalúan los planes de implantación de sistemas y las mejoras de éstos.
- Revisión de las instalaciones informáticas: incluyen la revisión de las políticas y procedimientos de personal, el cumplimiento de los estándares, seguridad, redes de comunicación y copias de seguridad.
- Revisión de las aplicaciones.
- Soporte a auditores no informáticos.

Asimismo, se pueden identificar cinco funciones vitales en una auditoría informática:

- Comprobar que se cumplen las normas y estándares vigentes en la organización.
- Velar por la eficacia y eficiencia del sistema informático.
- Verificar la calidad de los sistemas de información y proponer mejoras cuando sea necesario.
- Comprobar la seguridad de los sistemas de información.
- Supervisar controles internos existentes en la empresa.

4. 2 Áreas de una auditoría

Las áreas que deben ser revisadas en una auditoría dependerán de sus objetivos pero, en general, se identifican las siguientes:

- Comprobación del cumplimiento de requerimientos legales.
- Las políticas, normas, estándares y procedimientos aplicables en la organización.
- Protección de los activos (personas, instalaciones, redes, equipos, datos...). También se realiza un inventario y clasificación de éstos, y se identifica al responsable.
- Seguridad de los equipos, de las comunicaciones y redes. Internet, comercio electrónico y correo electrónico. Protección contra código malicioso.
- Mantenimiento de las instalaciones y equipos.
- Uso de mecanismos de cifrado y firma electrónica.
- Seguridad física (control de accesos físicos, protección ante desastres naturales y del entorno).
- Calidad del servicio y gestión de incidencias.
- Copias de seguridad y planes de continuidad.
- Control de accesos lógicos y gestión de privilegios.
- El acceso a los recursos, en especial por personas externas.
- Definición de funciones y obligaciones.
- Verificar en qué medida se cumplen los objetivos internos, los posibles riesgos y las metodologías utilizadas en su evaluación.
- Toda la empresa se involucra en el tema de seguridad, reciben formación y están mentalizados de su importancia.

4. 3 Auditoría externa y auditoría interna

Las auditorías pueden clasificarse de varias formas: según amplitud (total o parcial), frecuencia (periódica u ocasional), según el contenido, etc. En este apartado se han clasificado según el sujeto que realiza la auditoría: por tanto, las auditorías pueden ser internas o externas.

Ambas auditorías son compatibles y recomendables. Las características principales de cada tipo son:

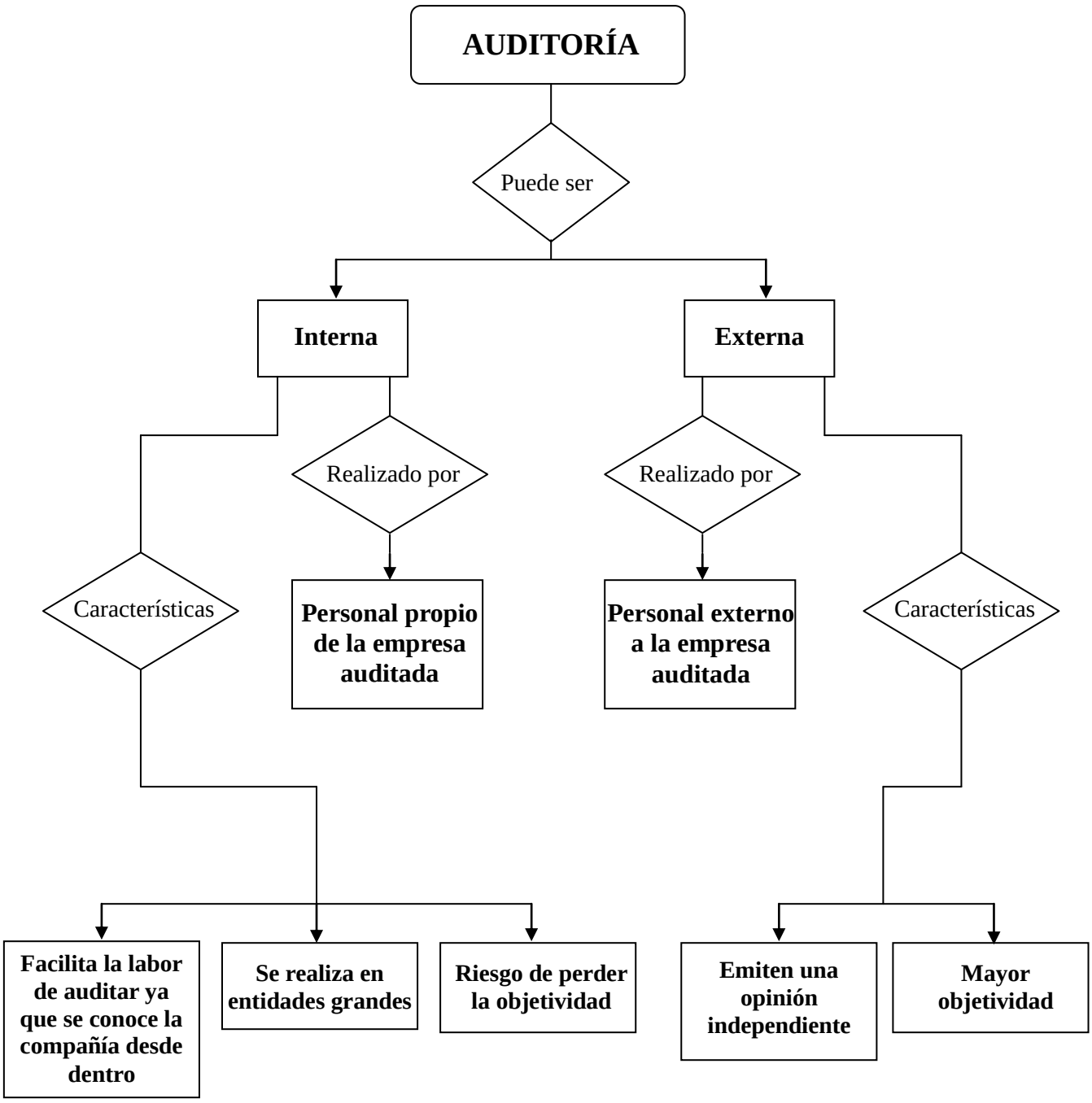
- **Auditoría interna**: es realizada por personal de la empresa auditada. Los auditores internos deben poseer la formación y experiencia suficiente. Estas personas conocen la organización desde dentro, lo cual facilita el trabajo de la auditoría pero existe el riesgo de que pierdan objetividad. Las relaciones personales entre los auditores y auditados no deben influir en los resultados de la auditoría.

  Generalmente este tipo de auditorías se realiza solamente en compañías grandes que pueden contar con los recursos humanos y económicos necesarios para llevarlas a cabo. Además, las auditorías internas pueden crearse por recomendación de una auditoría externa.

- **Auditoría externa**: es llevada a cabo por personas sin vinculación laboral con la compañía. Las entidades suelen solicitar este tipo de auditorías cuando identifican debilidades en la empresa como: mala imagen de la organización, clientes insatisfechos, dificultades económico-financieras, síntomas de descoordinación y desorganización, etc.

  La auditoría externa emite una opinión independiente sobre la situación de la empresa. Los auditores externos pueden apoyarse en los informes de la auditoría interna pero sin perder, ni un ápice, la objetividad.

Figura 4.1 Auditoría externa e interna



4. 4 Proceso de una auditoría

El proceso de una auditoría informática se puede desglosar en diferentes etapas y actividades que se explican a continuación:

- Estudio inicial de la auditoría
- Determinar los recursos necesarios
- Elaborar el plan de trabajo
- Actividades de la auditoría
- Informe final
- Carta de introducción del informe final

4. 4. 1 Estudio inicial de la auditoría

Es necesario definir de forma clara el **objetivo**, el **alcance** y la **profundidad** de la auditoría. El alcance define el entorno y los límites en que se desarrollará la auditoría informática. Esto es importante, sobre todo, en organizaciones grandes y dispersas. Se definen las materias, las funciones y las actividades a auditar y las que permanecerán fuera de la auditoría. En el final de esta etapa se determina la **viabilidad** de la auditoría. Si la auditoría es viable se continúa el proceso de auditar.

4. 4. 2 Determinar los recursos necesarios para auditar

Después del estudio inicial, se determinan los recursos económicos, materiales y humanos, necesarios para la realización de la auditoría. En cuanto a los recursos **económicos**, existirá un presupuesto que no debe excederse.

Una auditoría requiere una gestión lo más óptima posible. Para ello, es importante conseguir un equilibrio entre el cumplimiento de los objetivos de la auditoría, los plazos y el coste de la auditoría. La prioridad de estos tres factores debe ser el cumplimiento de los objetivos frente al presupuesto y el tiempo.

Los recursos **humanos** deben ser acordes con la auditoría a realizar. Es decir, la organización del equipo y el número de personas dependerá del entorno de la auditoría y de la formación de éstos. Además, se designa un líder (o líderes) en el equipo humano. El líder del grupo suele ser un auditor con gran experiencia.

En el equipo humano pueden diferenciarse las siguientes funciones:

- Gerente/s
- Jefe/s de equipo
- Auditor/es
- Auditor/es "*juniors*": estarán bajo la supervisión de auditores experimentados.

Los recursos **materiales** serán tanto *software* como *hardware*. El equipo de auditores elegidos debe conocer la organización de la empresa auditada. Para ello, el auditor observa entre otras cosas:

- ✓ El organigrama de la compañía
- ✓ Las relaciones entre los órganos de la entidad
- ✓ Los departamentos que la componen
- ✓ Los flujos de información
- ✓ Se comprueba que no existen puestos de trabajo distintos que realicen las mismas funciones
- ✓ Se evidencia que el número de personas asignadas a cada puesto es el adecuado.

Además, los auditores informáticos deben poseer un conocimiento previo de: el lugar geográfico donde se sitúan los sistemas, realizar un inventario de forma escrita que contenga la situación de todos los elementos lógicos y físicos que la empresa posee para su operación, la arquitectura *hardware* y *software* así como la configuración de los equipos, e informarse sobre las redes de comunicación utilizadas.

En cuanto a las aplicaciones utilizadas por la entidad auditada, se conocerá: la cantidad y complejidad de las aplicaciones, la documentación existente y la metodología utilizada en el desarrollo de las aplicaciones. Además, se obtendrá información sobre las bases de datos y los ficheros.

4. 4. 3 Elaborar el plan de trabajo

Se elabora el plan y los programas de trabajo. Para la elaboración del **plan de trabajo** es necesario conocer si la revisión se realiza por áreas generales cuya elaboración es más complicada y cara o si se realiza por áreas específicas. También se establecen las prioridades de materias que se auditan, se muestra las tareas que debe realizar cada miembro del grupo y se reflejan las ayudas que han de recibir los auditores por parte de los auditados.

El **programa de trabajo** detalla las actividades que se llevarán a cabo en la auditoría. Los auditores analizan el entorno y obtienen unas evidencias a través de análisis de información (recabada por el auditor o de otra índole) pruebas, entrevistas, cuestionarios, muestreos u otras técnicas y herramientas.

4. 4. 4 Actividades de la auditoría

Durante la auditoría es importante que exista una buena comunicación entre auditor y auditado. Los auditores tienen que recopilar y verificar información, y los auditados pueden servir de ayuda en esta tarea. Para obtener y comprobar la información los auditores cuentan con diferentes herramientas y técnicas que les facilitan el trabajo.

Las técnicas de auditoría informática tienen distintas finalidades, algunas se centran en comprobar el contenido de los ficheros de datos, otras están enfocadas en comprobar el buen funcionamiento del sistema y realizar pruebas sobre éste.

Algunas técnicas y herramientas que ayudar en la labor de auditar son:

- ⇒ Herramientas usadas: paquetes de auditoría, simuladores, estándares, monitores, cuestionarios *checklist*, cuestionarios generales y matrices de riesgo.
- ⇒ Técnicas de trabajo utilizadas por los auditores son: análisis de la información recabada del auditado y de la información propia, muestreo, simulación, entrevistas y pruebas.

Referente a las pruebas que realiza el auditor se puede distinguir entre pruebas de cumplimiento y pruebas sustantivas:

- Pruebas de cumplimiento: el auditor evidencia las debilidades existentes en los controles internos de la organización.
- Pruebas sustantivas: gracias a las cuales se comprueba la exactitud, validez e integridad de la información mediante la observación, muestreos, entrevistas, revisiones…

Durante todo el proceso de auditoría, el auditor elabora una extensa documentación por medio de las técnicas y herramientas utilizadas, y por los procedimientos seguidos. Toda esta documentación recopilada se conoce como los **papeles de trabajo** del auditor. Estos documentos justifican el trabajo realizado por los auditores.

Entre los requisitos que deben cumplir los papeles de trabajo destacan:

- ✓ Claridad: deben ser fáciles de entender y el auditor evitará los papeles manuscritos siempre que sea posible.
- ✓ Exactitud: el auditor debe mostrar cómo ha verificado las pruebas que contienen los papeles.
- ✓ Completos

Asimismo, los papeles de trabajo suponen un vínculo entre el trabajo realizado por el auditor con el informe final que le será entregado al cliente.

4. 4. 5 Informe Final

En la última etapa del proceso de la auditoría, se mantiene una reunión de cierre con los responsables de la empresa auditada con el fin de comunicarles los principales hallazgos de la actuación.

Después, los auditores comienzan a redactar el **borrador** del informe, que incluirá todas las evidencias, hallazgos, conclusiones y recomendaciones. El borrador o borradores que se elaboren se discuten con los auditados.

En último lugar, se elabora el **informe final**. El informe es el resultado por escrito de la evaluación realizada por los auditores sobre la situación de la entidad auditada. Siempre se realiza por escrito.

El informe reflejará fielmente y con imparcialidad los hechos reales descritos y de una forma clara y sencilla, entendible por la persona o personas a las que se dirige el informe. Se incluirá la información objetiva, los descubrimientos y las conclusiones respaldadas en los documentos de trabajo que evidencian los hechos.

Además, contendrá una descripción del trabajo que ha sido realizado y una valoración de la situación de la compañía señalando las debilidades que muestra, los riesgos a los que está expuesta y las posibles mejoras. También puede contener puntos positivos (si existen).

Asimismo, el informe deberá contener la fecha de elaboración y estar firmado por el auditor encargado del trabajo.

El informe consta de las siguientes partes:

- **Inicio** del informe:
  - Introducción: explicación de los antecedentes.
  - Objetivos, alcance y profundidad de la auditoría.
  - Agradecimientos (si procede).
  - Descripción del entorno informático.
  - Conclusiones.
  - Limitaciones (si han existido).
- **Cuerpo** del informe:
  - Metodologías y estándares utilizados.
  - Por cada área, se tratan los puntos que son objeto de mejora o de incumplimiento y se agrupan aquellos que son muy homogéneos.

    En cada punto incluir:

    ⇒ Descripción detallada de la deficiencia.

    ⇒ La causa y el efecto que tiene en la compañía.

⇒ Recomendación.

- Al final del informe se puede incluir un cuadro que facilite la priorización de los puntos y que facilite a la entidad dónde centrar sus esfuerzos:
  - ⇒ Riesgo estimado.
  - ⇒ Plazo de implantación.
  - ⇒ Posible coste asociado.
  - ⇒ La dificultad de implantación estimada.

- **Anexos**:
  - Entrevistas realizadas.
  - Cuestionarios utilizados y resultados.
  - Documentación utilizada.
  - Cualquier otro documento escrito o gráfico que pueda desviar la atención de la persona que lea el informe se incluye en este apartado.

4. 4. 6 Carta de introducción del informe final

La **carta de introducción** o de presentación del informe definitivo resume la auditoría que ha sido realizada. Proporciona una conclusión general mostrando las debilidades más importantes (sin incluir recomendaciones).

Esta carta no sobrepasa las cuatro páginas e incluye la fecha, naturaleza, objetivos y el alcance de la auditoría. El destinatario de la carta será el responsable de la empresa o la persona que encargo la auditoría.

4. 5 El auditor

El auditor es la persona encargada de llevar a cabo el proceso de la auditoría. El auditor recaba toda la información necesaria para emitir de forma objetiva un juicio global, basándose en evidencias (hechos demostrables).

Los auditores deben poseer una serie de cualidades importantes para desempeñar su trabajo de forma apropiada. Entre sus cualidades se pueden destacar:

- **Cualidades extrínsecas**:
  - ✓ Neutralidad
  - ✓ Objetividad
  - ✓ Independencia
  - ✓ Imagen
  - ✓ Reputación
  - ✓ Seguridad en sí mismo
  - ✓ Madurez
  - ✓ Responsabilidad
  - ✓ Interés
  - ✓ Integridad
  - ✓ Ética
- **Cualidades intrínsecas**:
  - ✓ Creatividad
  - ✓ Imaginación
  - ✓ Capacidad de análisis
  - ✓ Capacidad de síntesis
  - ✓ Estabilidad emocional
  - ✓ Sensatez de juicio
  - ✓ Tenacidad
  - ✓ Persistencia

Los auditores informáticos deben tener lógicamente, una **formación** y **experiencia** en auditoría e informática. Poseerá la capacidad de poder comprender la terminología informática y de entender manuales realizados por personal técnico. El auditor contará además, con la suficiente formación para comprobar que los controles de cada actividad son los correctos.

El auditor informático debe estar al día sobre las nuevas tecnologías de *software* que surgen en el mercado. Asimismo, debe ser capaz de comprobar que la organización cuenta con la cantidad de equipos y de *software* necesarios para desempeñas sus tareas, que estos recursos son los adecuados y que el acceso a éstos es controlado.

Por otro lado, un auditor informático debe poseer algunos **conocimientos** fundamentales para desempeñar su trabajo, como:

- Situar correctamente la función de la informática en la estructura de la organización, es decir, el auditor tiene que ser capaz de determinar si el área de informática depende del nivel jerárquico apropiado.
- Conocer procedimientos y técnicas para auditar.
- Capacidad de identificar los riesgos a los que los elementos informáticos y las personas relacionadas se enfrentan.
- Habilidad para identificar las funciones de cada puesto de trabajo en el área de informática y comprobar el cumplimiento de dichas funciones.
- Ser capaz de evaluar las tareas que deben ejecutarse para que el procesamiento electrónico de datos sea adecuado.

El auditor ha de conocer también la legislación, reglamentos, normas y cualquier otro documento necesario para llevar a cabo una auditoría. Por tanto, tiene que tener conocimiento de:

⇒ Las normas: pueden ser leyes, directrices de la dirección...

⇒ Las herramientas de control: el auditor debe conocerlas para poder desempeñar su trabajo.

⇒ Los objetivos de la empresa: de la compañía, de las áreas a auditar, los departamentos...

⇒ El alcance de la auditoría: las actividades implicadas, el personal...

⇒ Los hechos reales: comprobados por el auditor con la certeza de que no se ha equivocado.

⇒ Las causas y los efectos: identificar las causas y los efectos de los hechos y situaciones.

⇒ La comunicación: entre el auditor y el auditado.

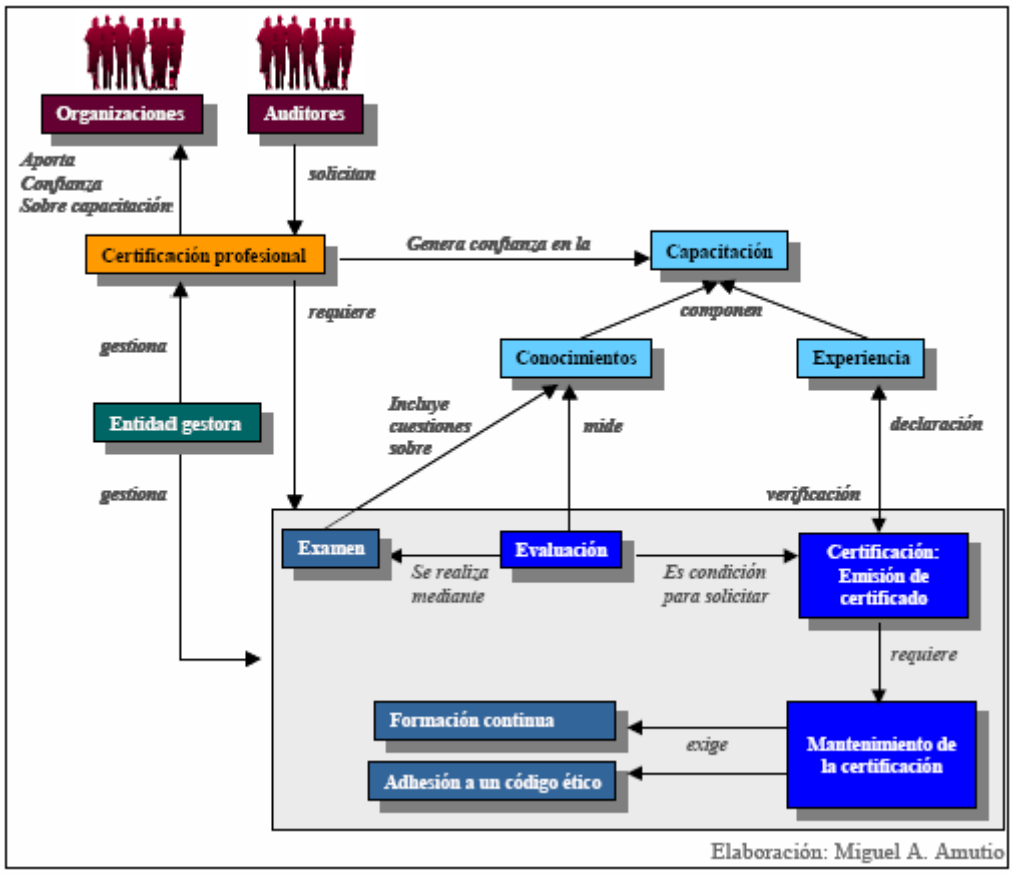
⇒ Las técnicas modernas: el auditor debe estar al día de los métodos existentes que surgen que les ayude en su trabajo.

Desde 1978, **ISACA** (Information *Systems Audit and Control Association*) emite un certificado profesional como auditor de sistemas **CISA** (*Certified Information Systems Auditor*). Para obtenerlo es necesario aprobar un examen, contar con la experiencia profesional suficiente y aceptar un código de ética profesional.

Para finalizar este apartado referente a los auditores, comentar que la **ISACF** (*Information Systems Audit and Control Foundation*) es la Fundación de Control y Auditoría de Sistema de Información propone el siguiente Código de Ética Profesional que deben cumplir los auditores:

1. Promover en las auditorías de sistemas de información, el establecimiento y acatamiento de procedimientos, normas y controles.
2. Cumplir con las normas de auditoría de sistemas de información que adopte la ISACF.
3. Servir con lealtad, diligencia y honestidad a los empleadores, accionistas, clientes y público en general. No intervenir de forma consciente, en actividades ilegales o impropias.
4. Conservar la confidencialidad de la información conseguida que no debe ser utilizada en beneficio propio o divulgada a terceros no pertinentes.
5. Desempeñar sus funciones de manera objetiva e independiente.
6. Mantener su competencia en materias que afecten a la auditoría y sistemas de información.
7. Las conclusiones y recomendaciones obtenidas en el proceso de auditar deben obtenerse y documentase con el material suficiente.
8. Informar a las partes implicadas del resultado del proceso de auditoría realizado.
9. Fomentar la formación de la dirección, clientes y público en general, para mejorar su comprensión en relación a la auditoría y los sistemas de información.
10. Conservar altos estándares de conducta y carácter en las actividades profesionales y privadas.

Figura 4.2 Certificación profesional de un auditor



Fuente: Módulo "*Confianza en los sistemas de información y Criterios de Seguridad, Normalización y Conservación de las aplicaciones usadas en el ejercicio de Potestades*", II Curso de Auditorías de Sistemas de Información (INAP), impartido por Miguel Ángel Amutio Gómez en 2006.

4. 6 Herramientas y técnicas

Para llevar a cabo una auditoría, el uso de herramientas y técnicas facilita considerablemente el trabajo al auditor. A continuación, se detallan las principales:

- **Entrevista**: El auditor entrevista al auditado con alguna finalidad concreta. Se recaba mucha información que posiblemente no se obtendría por otros medios.

  La entrevista se realizará sin tensión y de manera correcta. El auditor evitará dar sensación de interrogatorio y utilizar jergas que puedan dificultar el entendimiento de la pregunta realizada. Igualmente, el entrevistado no usará jergas que el auditor no comprenda.

  El auditado ha de sentirse lo más cómodo posible y el entrevistador debe inspirar confianza. Además, las preguntas que formule el entrevistador no deben conducir a la respuesta.

  Los auditores deben tener la capacidad de captar información no verbal, como gestos realizados por el entrevistado, las posturas, los silencios... y reacciones del entrevistado ante determinadas preguntas.

  El auditor selecciona a qué funciones entrevistará. Pueden ser: directivos, jefes de proyecto, analistas, programadores, usuarios, técnicos de sistemas, administradores de bases de datos, auditores internos (si se trata de una auditoría externa), responsables de seguridad, responsables de desarrollo... o cualquier función de la organización que le aporte información relevante.

  Después de elegir la persona (o personas) a entrevistar, se debe elegir la fecha, hora y el lugar. El auditor evitará la hora de la comida, la primera hora o el final de la jornada. Respecto al lugar, es preferible que el lugar donde se realice la entrevista sea un despacho o una sala de reuniones aislados. Además, es deseable avisar con antelación a la persona aunque, en ocasiones, es imprescindible el **factor sorpresa**.

  Finalmente, el auditor realizará un resumen de la entrevista y, en un futuro, podrá ampliar la entrevista al auditado.

- **Cuestionario**: Los auditores realizan una serie de cuestionarios a los auditados que, utilizados de forma correcta, pueden explicar cómo ocurren los hechos y las situaciones. Un buen auditor elabora muchas veces sus cuestionarios según el área y la organización que audita.

Los cuestionados deben ser muy específicos para cada área de la empresa auditada y para cada situación. Someter al auditado a preguntas estereotipadas no ayudará demasiado en la realización de la auditoría. Los cuestionarios han de adaptarse a cada situación para que sean una herramienta útil. Además, las preguntan de los cuestionarios pueden agruparse por temas.

El conjunto de las preguntas es lo que se conoce como ***checklist***. Generalmente las *checklists* se contestan oralmente. Es importante la manera de formular las preguntas y el modo. El auditado debe responder de forma escueta y clara. El auditor sólo interrumpirá cuando las respuestas no se ajusten a las preguntas o desee una aclaración de la respuesta. Determinadas preguntas de especial transcendencia han de repetirse, formuladas de manera distinta para comprobar si existen contradicciones.

El auditor toma notas delante del auditado. Un buen cuestionario proporciona gran ayuda en el proceso de una auditoría pero es más importante la capacidad del auditor.

Las *checklists* pueden ser:

- *Checklist* de rango: las preguntas se puntuar dentro de un rango preestablecido. Por ejemplo, el rango puede comprender los valores desde 1 (como valor más desfavorable) a 5 (como valor más positivo); o de 1 a 10.
- *Checklist* binaria: las preguntas tienes como respuesta si o no, lo que aritméticamente equivale a un 1 o un 0.

- **Trazas**: El auditor informático verifica los programas de la compañía auditada y comprueba si éstos realizan solamente las funciones previstas. Para llevar a cabo esta tarea, se utilizan productos *software* que comprueban cuales son los caminos que siguen los datos a través del programa.

  En una traza se comprueba que la ejecución y resultado de un programa es adecuado, haciendo un seguimiento de dicha ejecución y las validaciones de datos llevados a cabo.

  Una traza es un registro histórico de todos los cambios realizados junto con la información del usuario que realizo la modificación y la fecha. Las trazas no modifican el sistema. Si estas trazas sobrecargan el sistema, se prevé las fechas y horas más apropiadas para utilizarlas.

Los registros o *logs* son historiales que muestran los cambios realizados en la información (adición, borrado o modificación) y cómo se ha producido ese cambio.

- **Observación**: es muy útil cuando se observa sin que el personal de organización auditada sepa que se trata del auditor. La observación puede contrariar las respuestas en las entrevistas y cuestionarios.

  Por ejemplo, si los entrevistados han afirmado que a determinadas áreas no accede personal no autorizado, y el auditor observa que no existe ningún tipo de control de accesos, se produce una contradicción con la información manifestada por el auditado.

- **Flujogramas**: se utilizan para representar gráficamente procesos realizados. Permite plasmar las entradas, las salidas que se producen, los procesos o funciones que recorre.

  Los diagramas de flujos pueden mostrar controles utilizados en la compañía, las autorizaciones, la segregación de funciones, etc. o cualquier proceso que interese reflejar a través de esta herramienta.

- **Muestreo estadístico**: las muestras pueden referirse al control de visitas, a la alteración de documentación, a la revisión de programas… y cualquier otra información que probablemente no sea viable analizar al 100% de la "población" por lo que se analiza una muestra representativa.

  El mayor inconveniente es que el resultado podría diferir si la muestra hubiera sido completa. Se debe encontrar un equilibrio entre el coste o esfuerzo y una fiabilidad aceptable. Además, se puede hacer uso de paquetes estadísticos.

- **CAATs** (*Computer Asisted Audit Techniques*): o TAAOs (Técnicas de Auditoría Asistida por Ordenador) son un conjunto de técnicas que utilizan herramientas informáticas a lo largo de todo el proceso de auditoría.

4. 7 Controles internos

Un control es una actividad o acción cuyo fin es prevenir, detectar y corregir errores o anomalías que puedan trastornar el funcionamiento normal de un sistema en relación a la consecución de sus objetivos.

El informe **COSO** (las siglas COSO corresponden al *Committee of Sponsoring Organizations of the Treadway Commission, National Commission on Fraudulent Financial Reporting*) definen el control interno como: "*un proceso efectuado por el Consejo de Administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:*

- eficacia y eficiencia de las operaciones,

- fiabilidad de las operaciones financieras,

- cumplimiento de las leyes y normas que le sean aplicables".

Los controles deben ser: fiables, lo menos complejos posible, adecuados, revisables y rentables. Los controles son responsabilidad de la dirección, deben realizarse por personal cualificado y verificados por auditores. Los auditores evalúan los controles existentes en la organización, recomiendan la implantación de nuevos controles, refuerza aquellos que lo necesiten y, en raras ocasiones, recomienda su supresión.

Los controles internos pueden clasificarse de diversas formas según:

- Su **frecuencia**:
  - Continuo
  - Periódico
  - Esporádico
- Su **naturaleza**:
  - Generales: controles organizativos y operativos, de *hardware*, de *software*, de desarrollo y mantenimiento de aplicaciones, de acceso, de procedimiento.
  - De Aplicación: controles de entrada, salida, de proceso.

- El **período en que operan**:
  - Preventivos: actúan "a priori".
  - De detección: reflejan acciones o actividades no adecuadas.
  - Correctivos: se aplican "a posteriori" para rectificar errores.
  - De recuperación: facilitan la vuelta a la normalidad después de producirse un error o interrupción.

Por otro lado, en el marco de control de las Tecnologías de la información es importante mencionar la metodología **COBIT** (*Control Objectives for Information and related Technology*), desarrollada por la asociación ISACA (*Information Systems Audit and Control Association*) e ITGI (*IT Governance Institute*)

COBIT es un conjunto de buenas prácticas para el control de la información, las tecnologías de la información y los riesgos que conllevan. COBIT versión 4.1 consta de 34 objetivos de alto nivel agrupados en cuatro **dominios**:

- Planificación y Organización: identifica la forma en que las tecnologías de la información ayudan a alcanzar los objetivos de la empresa. Destaca la implementación de una estructura organizacional y una estructura tecnológica adecuada para alcanzar unos resultados óptimos.
- Adquisición e Implementación: Identificación, implementación e integración de las soluciones de TI (tecnología de información), ya sean desarrolladas o adquiridas en los procesos del negocio. También se destaca el mantenimiento y el cambio que una entidad debe adoptar para garantizar que las soluciones sigan cumpliendo los objetivos.
- Entrega y Soporte: Se preocupa de la entrega de los servicios requeridos. Cubre diversos aspectos relacionados con la seguridad y la continuidad, los usuarios del servicio, la administración de los datos y las instalaciones operacionales.
- Supervisión y Evaluación: evalúa la calidad y cumplimiento de los requerimientos de control en los procesos de TI.

Una auditoria de los sistemas de una entidad se considera completa si abarca los 34 objetivos de control que se describen en la metodología COBIT. Los **requerimientos** de negocio para la información que se aplican a los objetivos son:

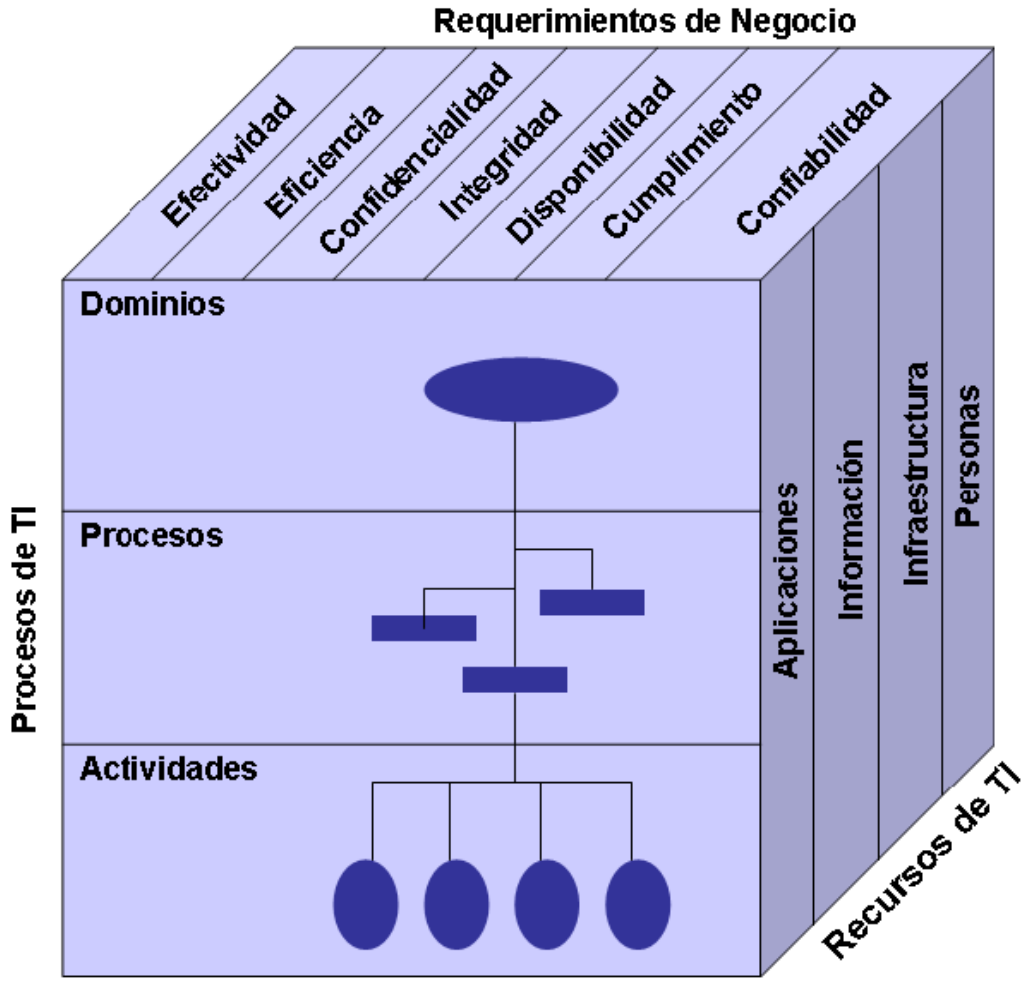
- ✓ Eficacia.
- ✓ Eficiencia.
- ✓ Confidencialidad.
- ✓ Integridad.
- ✓ Disponibilidad.
- ✓ Cumplimiento de la legislación o normativa.
- ✓ Confiabilidad o fiabilidad.

Finalmente, los **recursos** de las TIC (Tecnologías de información y comunicación) que pueden identificarse en COBIT son los siguientes:

- o Datos
- o Aplicaciones
- o Tecnología
- o Instalaciones
- o Personal

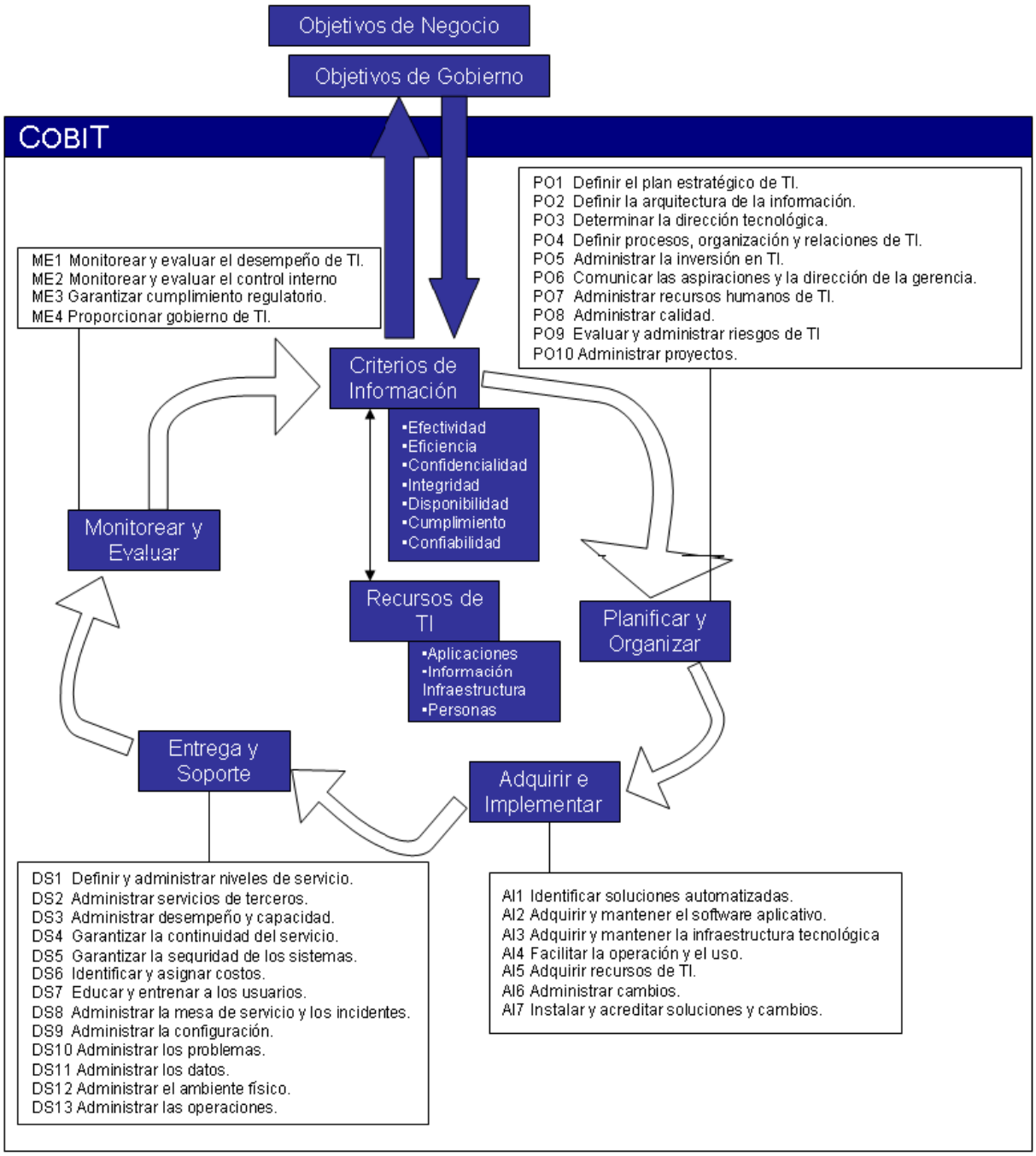
Los procesos de TI manejan diferentes recursos de TI que respondan a los requerimientos del negocio con el fin de lograr unas metas de TI. A continuación, se ilustran estos conceptos en el *cubo de COBIT*.

Figura 4.3 Cubo de COBIT



Fuente: COBIT 4.1 (versión en español). Figura 22.

Figura 4.4 Marco de trabajo de COBIT



Fuente: COBIT 4.1 (versión en español). Figura 23.

V. CUESTIONARIO

5. 1 Introducción

En apartados anteriores, se comentó la importancia de los cuestionarios en la realización de auditorías. En este capítulo, se detalla un cuestionario de auditoría informática de la seguridad lógica. El cuestionario consta de una serie de preguntas agrupadas por bloques. Las preguntas han sido recopiladas de los temas tratados en este documento.

Algunas preguntas son de respuesta binaria y otras de rango con valores comprendidos entre 0 y 5. En las respuestas binarias, habrá casos que no se ajuste a una ni a la otra, pero el auditor deberá **adaptar** el cuestionario según el área y la organización que audita. Por lo tanto, esto es un posible modelo de cuestionario y será útil para algunas auditoría y para otras no dependiendo de la compañía a auditar.

Las respuestas tienen un peso que ayudarán a conocer el grado de seguridad lógica aplicado en la compañía. Las respuestas con peso 5 aquellas más favorables y siendo 0 la opción más desfavorable. Existen respuestas con respuesta única o múltiple, dependiendo del tipo de pregunta.

Al finalizar un bloque de preguntas, se elabora unas recomendaciones que la organización debería implantar para mejorar la seguridad lógica y de accesos, junto con una estimación del nivel de riesgo a la que se enfrenta la entidad y su puntuación en el cuestionario.

La puntuación mínima obtenida es 0 y la máxima dependerá del número de preguntas de las que conste el bloque de preguntas. Si existe alguna respuesta que expone que la pregunta no es aplicable, este hecho influirá en la máxima puntuación restándole el valor de la pregunta no aplicable si esa respuesta es marcada. A mayor puntuación, menor riesgo para la empresa.

El cuestionario servirá de ayuda al auditor durante el desarrollo de la auditoría. Se puede entregar el cuestionario a los auditados para que contesten a las preguntas o el auditor podrá ir formulando las preguntas oralmente al auditado.

En "*Anexos*" se adjuntan dos tablas: una tabla contiene las preguntas agrupadas por temas y sus respectivas respuestas con sus pesos asignados; y la otra muestra las preguntas con las respuestas asociadas a una recomendación.

Si el cuestionario se va a entregar en papel a un auditado para que él lo realice, no deberá contener los pesos asignados a las respuestas para que no influya en sus contestaciones.

5. 2 Aplicación informática

Se ha elaborado una aplicación informática para implementar el cuestionario y facilitar así el trabajo a los auditores. La aplicación permite contestar de forma interactiva y obtener en el momento los resultados y recomendaciones a aplicar.

La aplicación es un **prototipo** para demostrar la idea y su viabilidad que podría mejorarse. Están implementados todos los apartados de preguntas pero se podrían **ampliar** o añadir nuevos temas. También se podrían asignar pesos a las preguntas o incluso a los temas según la empresa que se audite, el sector, etc. Asimismo, en recomendaciones se podrían asignar pesos según el nivel de importancia de dicha recomendación.

En aquellas preguntas de respuesta única aparece la primera **opción premarcada** por el mero hecho de facilitar el trabajo al usuario de la aplicación y sin pretender que éste crea que es la opción más acertada.

Las preguntas están enfocadas para un conjunto de empresas que pudieran hacer uso del cuestionario. En cambio, existirán otras entidades que no podrán utilizarlo debido a que las respuestas no se ajustarán a su situación.

El cuestionario podría rellenarse directamente sobre la aplicación o cuando sea más cómodo rellenarlos en papel y después, introducir las respuestas obtenidas en la aplicación informática para que muestre los resultados.

En determinados apartados como en "*Control de Acceso Lógico*" si no existen controles de acceso lógicos a los sistemas de información el cuestionario finaliza en ese momento, no pudiendo contestar las siguientes preguntas ya que son referidas a los controles de acceso lógicos existentes en la organización. En dicho caso, se mostrará una ventana que recomienda al usuario la implantación de dichos controles.

Al finalizar cada bloque de preguntas se muestran unas recomendaciones sobre dicho tema. Se muestra el nivel de riesgo al que se enfrenta la entidad y dependiendo de riesgo se visualiza de distinto color:

- Si el riesgo es alto aparece la palabra "*Alto*" en rojo.
- Si el riesgo es medio aparece la palabra "*Medio*" en naranja.
- Si el riesgo es bajo aparece la palabra "*Bajo*" en verde.

También aparece una puntuación comprendida entre 0 y la puntuación máxima del bloque. Asimismo, aparecen todas las recomendaciones que debería llevar a cabo la organización para reducir el riesgo. Si no existen recomendaciones se mostrará un mensaje de enhorabuena.

Durante la realización del cuestionario sobre un determinado tema el usuario sabrá en todo momento en que punto se encuentra del proceso gracias a una barra de progreso. De esta forma, puede hacerse una idea de cuantas pantallas le faltan para finalizar el cuestionario.

Además, es posible navegar por las pantallas haciendo uso del teclado pulsando "Alt + primera letra". En la primera pantalla, en menú, aparecen varias palabras que comienzan por "c" o "p". En ese caso, se ha utilizado las siguientes combinaciones de teclas:

- Para acceder a "*Contraseñas*" se utiliza "Alt + c"
- Para acceder a "*Copias de Seguridad*" se utiliza "Alt + o"
- Para acceder a "*Control de Acceso Lógico*" se utiliza "Alt + n"
- Para acceder a "*Política de seguridad*" se utiliza "Alt + p"
- Para acceder a "*Programas*" se utiliza "Alt + r"

Pulsado la tecla "Alt" aparece subrayada la letra clave de acceso para la navegación por teclado.

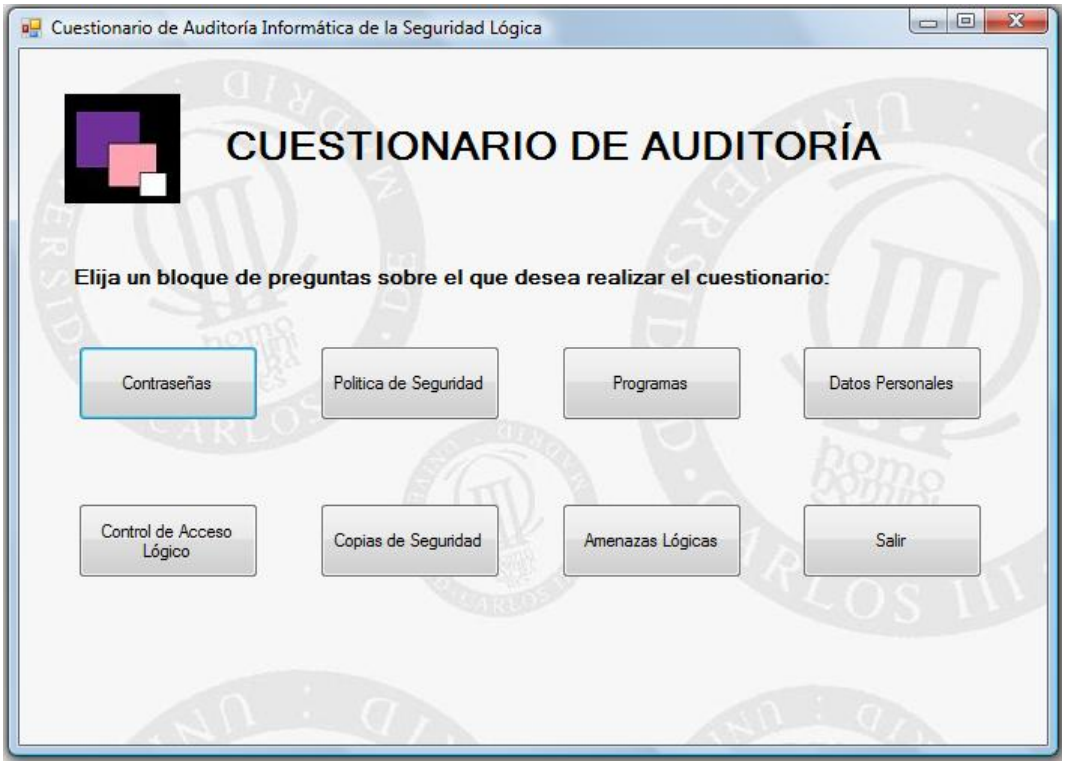
Con el botón "anterior" y "siguiente" el usuario podrá ir a la pregunta anterior o posterior respectivamente y se quedará guardada la opción que había marcado hasta finalizar el proceso, es decir, hasta que se muestran las recomendaciones.

5. 3 Manejo de la aplicación

La aplicación está desarrollada en *Microsoft Visual Basic 2008* bajo el sistema operativo *Windows Vista*. Para comenzar a utilizarla es necesario hacer doble clic en el fichero ejecutable.

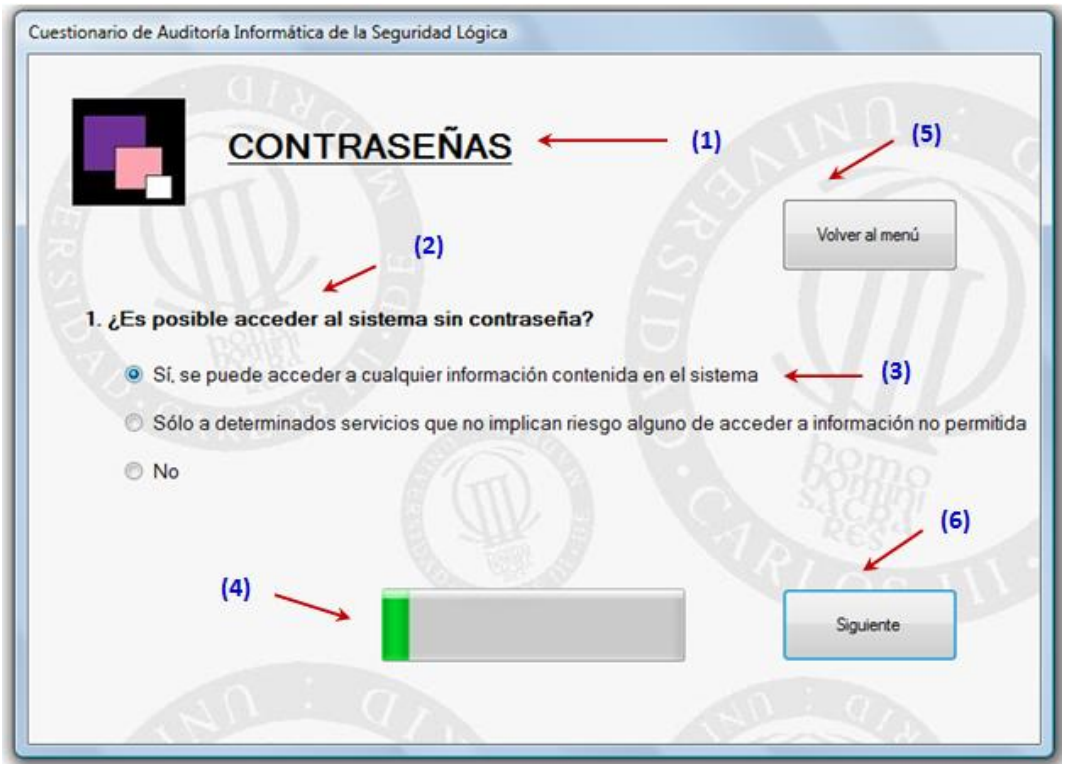
Inicialmente, se muestra un menú con los temas que contiene el cuestionario (Figura 5.1).

Figura 5.1 Ejemplo Pantalla 1



Si se pincha sobre contraseñas, se visualiza la siguiente pantalla (Figura 5.2). Se puede observar el nombre del bloque de temas (1), la pregunta (2), las respuestas siendo la primera la premarcada (3) por defecto y la barra de progreso (4) para que el usuario sepa en qué punto del proceso se encuentra. Además, la pantalla muestra dos botones, uno para volver al menú (5) y otro para acceder a la siguiente pregunta (6).

Figura 5.2 Ejemplo Pantalla 2



Si se pulsa el botón siguiente (figura 5.2 (6)) se visualiza la segunda pregunta sobre contraseñas. En esta pantalla (Figura 5.3) aparece un nuevo botón (1) utilizado para retroceder a la pregunta anterior.

Figura 5.3 Ejemplo Pantalla 3

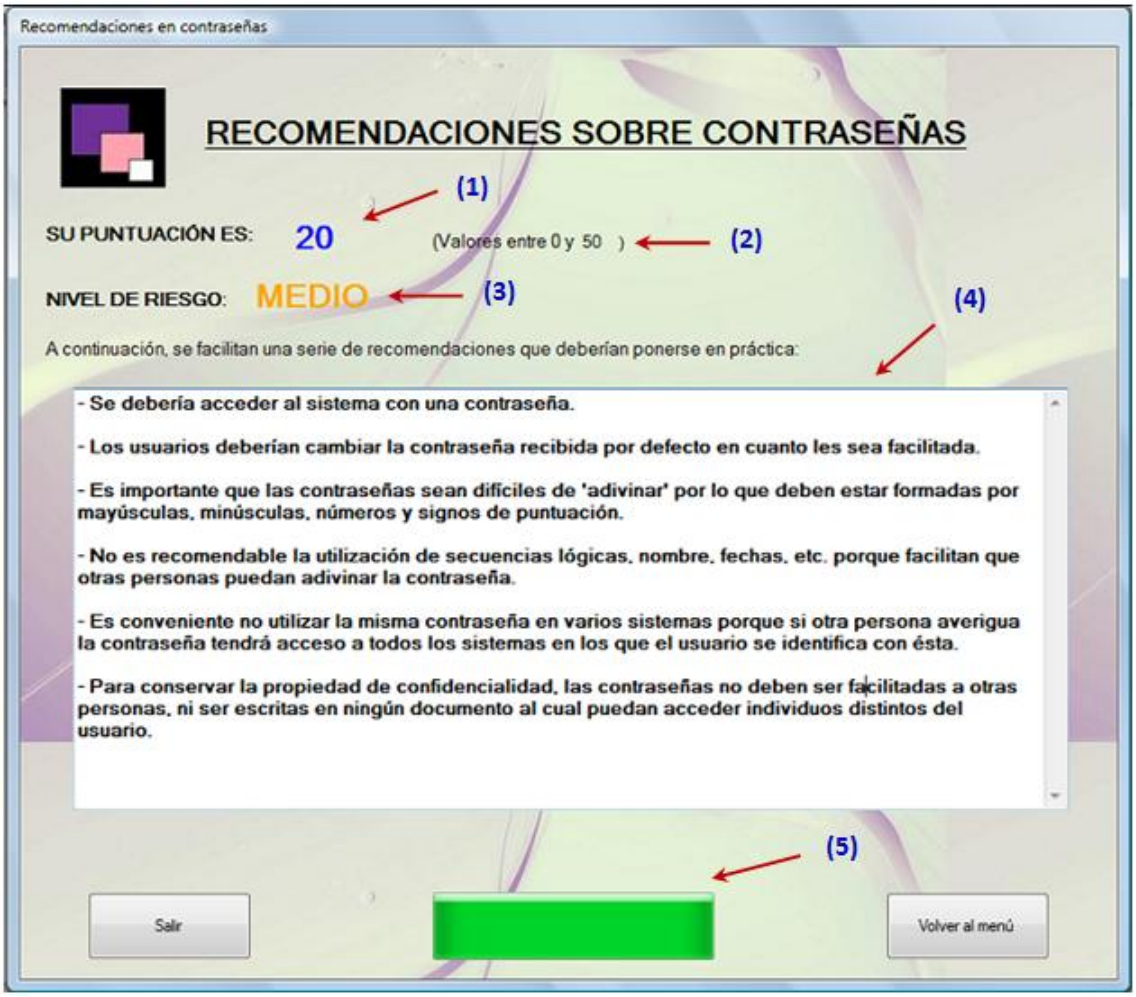
Al llegar a la última pregunta del bloque (Figura 5.4), aparece un botón (1) que si se hace clic sobre el mismo se mostrarán las recomendaciones.

Figura 5.4 Ejemplo Pantalla 4

En la pantalla de recomendaciones (Figura 5.5), se puede observar la puntuación obtenida (1) por el usuario de la aplicación después de completar todas las cuestiones sobre contraseñas. A la derecha de la puntuación, se muestra los valores mínimos y máximos (2) que podrían obtener al completar el bloque de preguntas. Debajo de la puntuación se indica el nivel de riesgo (3) al que está sometida la organización. En la figura 5.5 el nivel de riesgo es medio, por ese motivo aparece de color naranja.

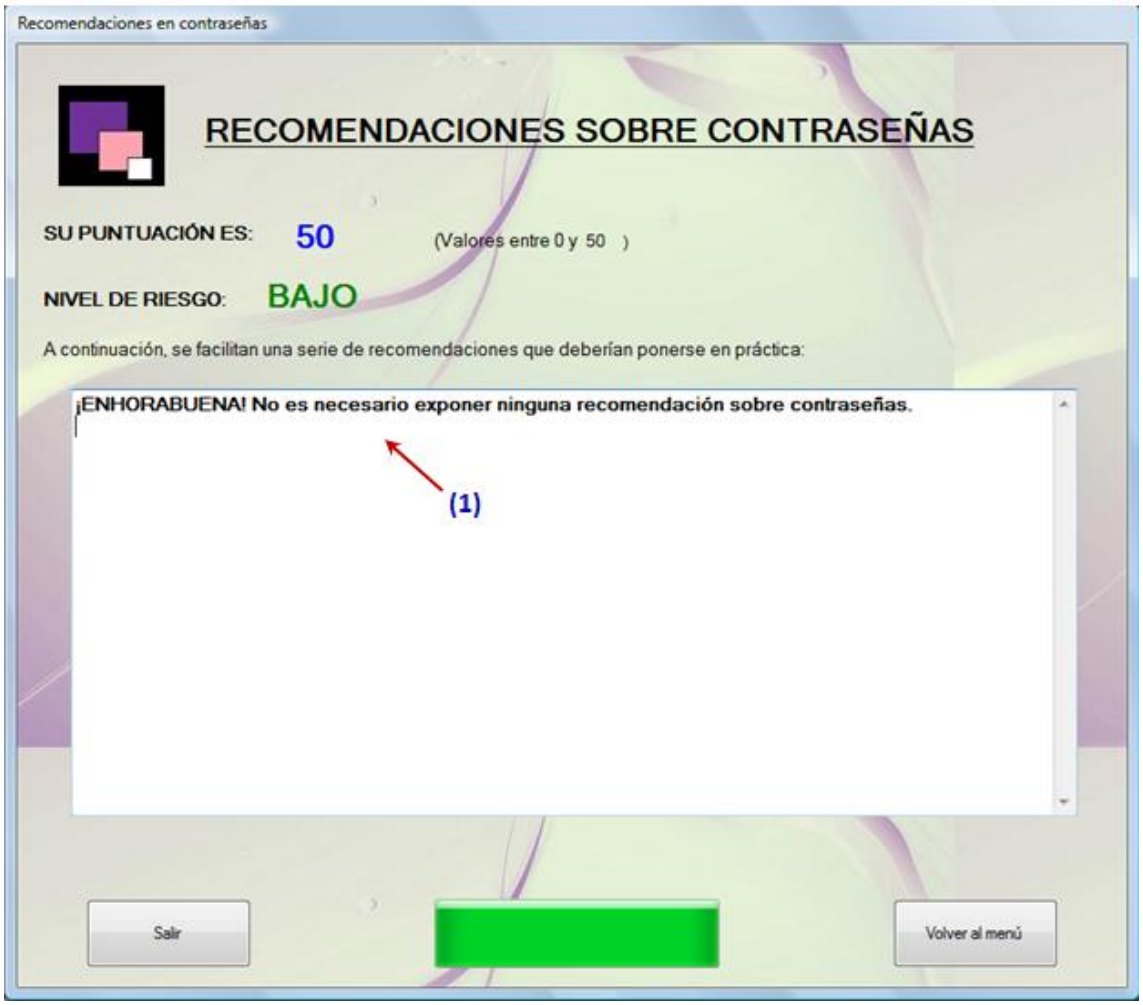
Asimismo, se visualizan las recomendaciones (4) que se debería poner en práctica para reducir el riesgo de que se pudiera materializar un daño en la empresa. La barra de progreso (5) se muestra completa ya que se ha finalizado el proceso.

Figura 5.5 Ejemplo Pantalla 5



En el caso que no fuese necesario realizar ninguna recomendación, la pantalla (Figura 5.6) mostraría un mensaje de felicitación (1). El nivel de riesgo es bajo y aparece de color verde.

Figura 5.6 Ejemplo Pantalla 6



5. 4 Casos prácticos

En sucesivos apartados se expondrán una serie de casos prácticos imaginarios referentes a empresas que hacen uso de la aplicación. De esta forma, se podrá mostrar el funcionario del cuestionario de auditoría y facilitar su comprensión.

5. 4. 1 Caso práctico: Contraseñas

La empresa "X" cuenta con 200 empleados que utilizan siempre un identificador y contraseña para validarse en su sistema. La compañía les obliga a que la longitud mínima de sus contraseñas sea de ocho caracteres y que los empleados se identifiquen individualmente.

La organización también exige que la contraseña sea cambiada una vez al mes pero no controla que los usuarios utilicen contraseñas usadas anteriormente. Existen empleados que utilizan nombres, fechas o teléfonos para recordar fácilmente su *password*. Algunos trabajadores utilizan contraseñas usadas también en otros sistemas.

A los usuarios no se les facilita contraseñas por defecto para evitar que por pereza u otro motivo no las cambien. Además, se les advierte de la importancia de no facilitar su contraseña a otros usuarios, escribirla o almacenarla en su ordenador para evitar que terceros la intercepten.

La organización se somete a una auditoría y se dispone a contestar el cuestionario aportado por el auditor. En el apartado de "*Contraseñas*", sus respuestas han sido las siguientes:

Figura 5.7 Contraseñas 1

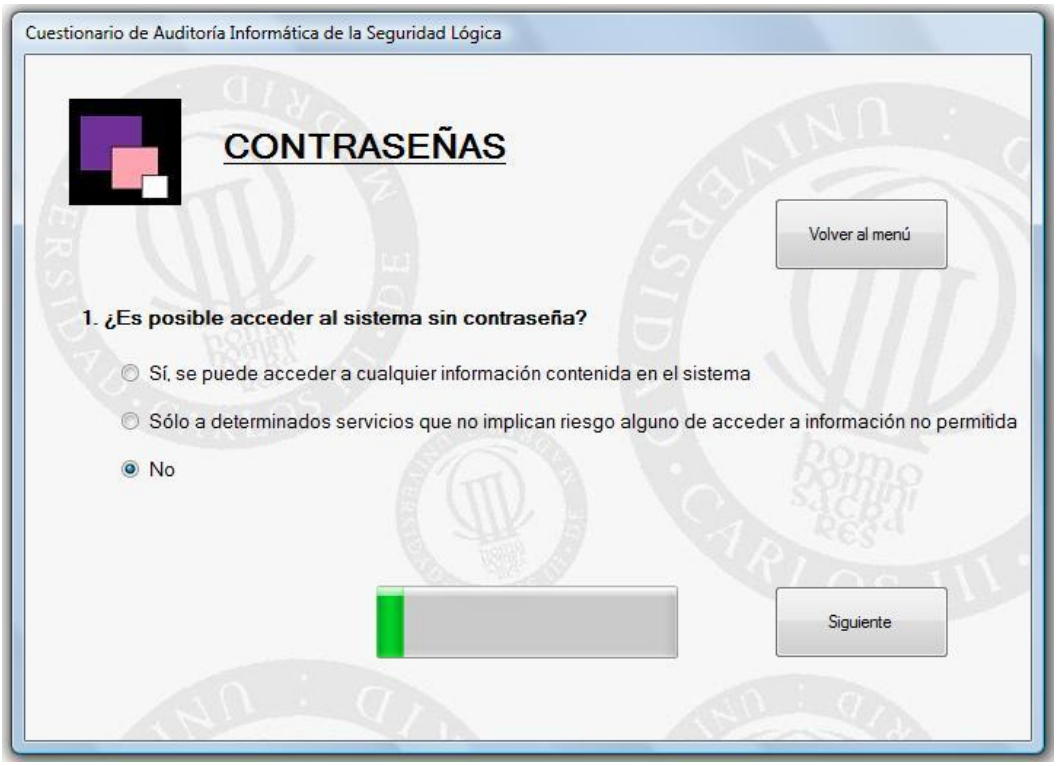


Figura 5.8 Contraseñas 2

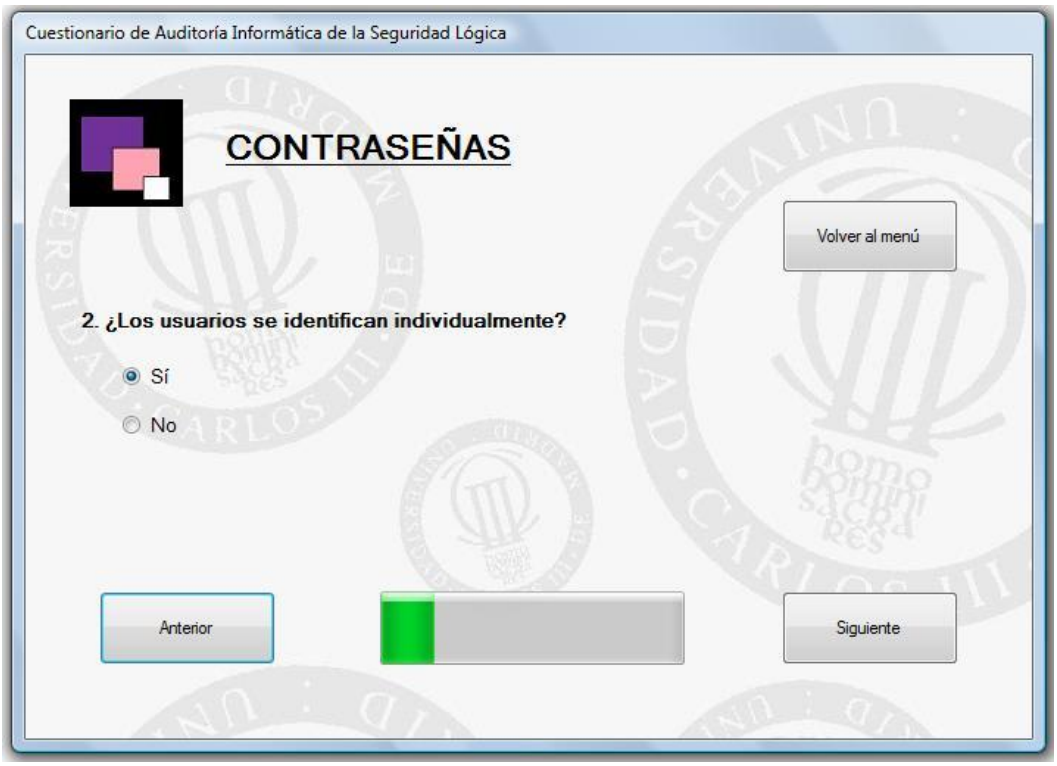


Figura 5.9 Contraseñas 3

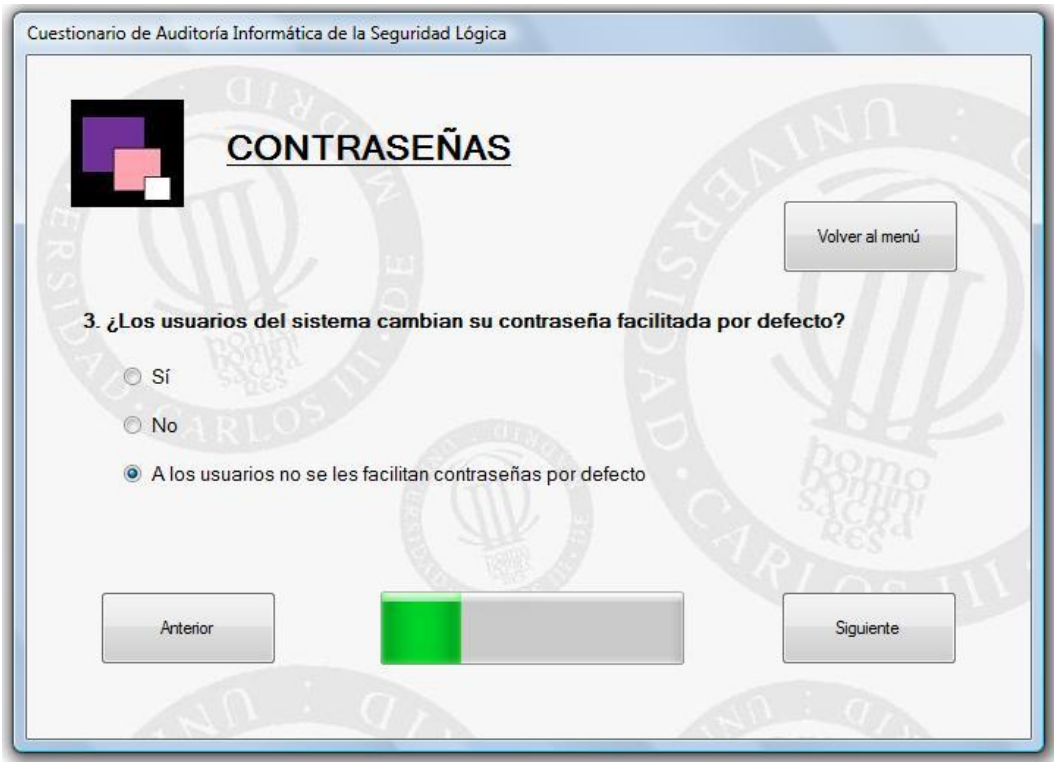


Figura 5.10 Contraseñas 4

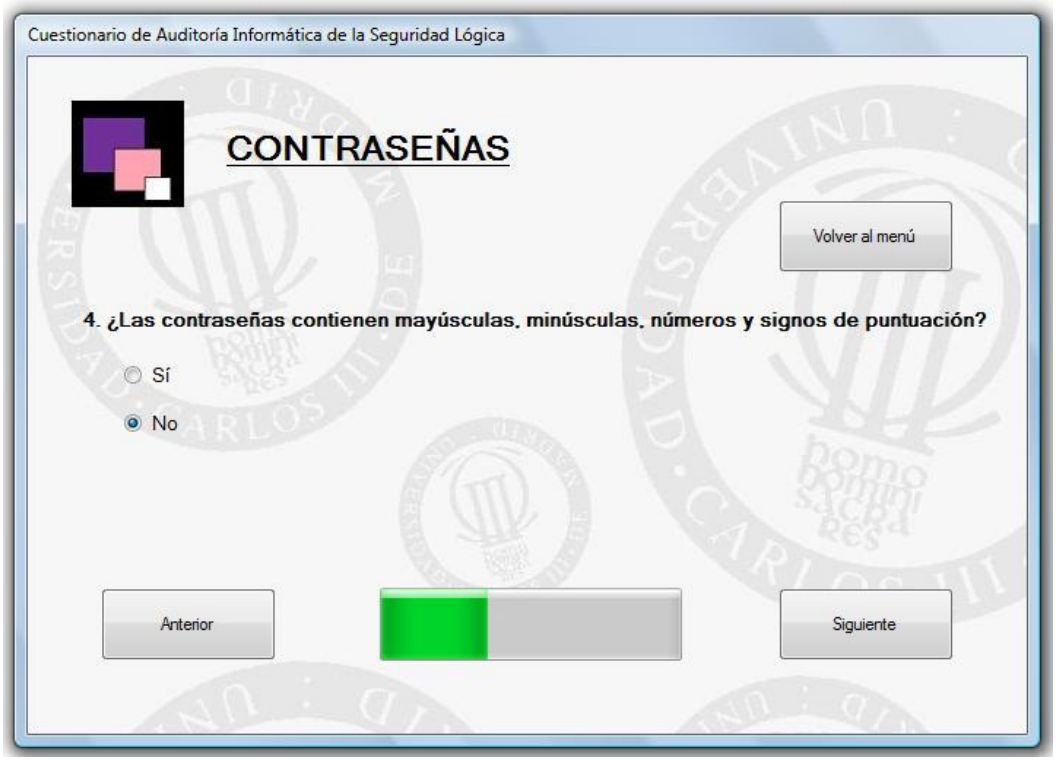


Figura 5.11 Contraseñas 5

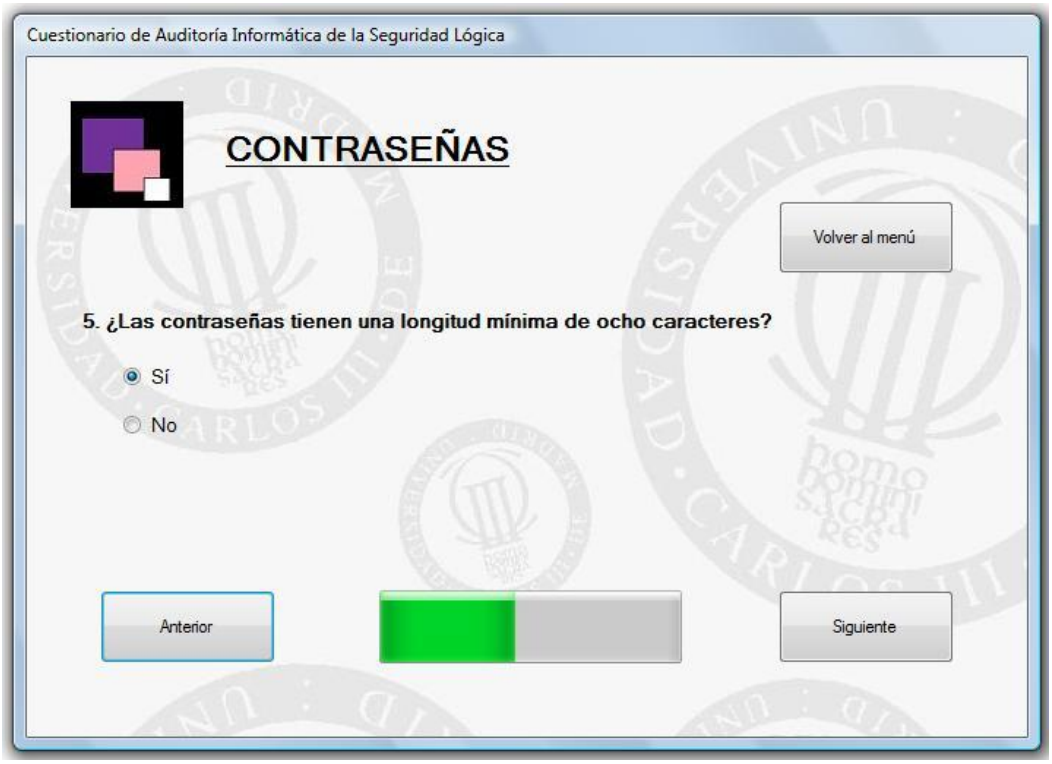


Figura 5.12 Contraseñas 6

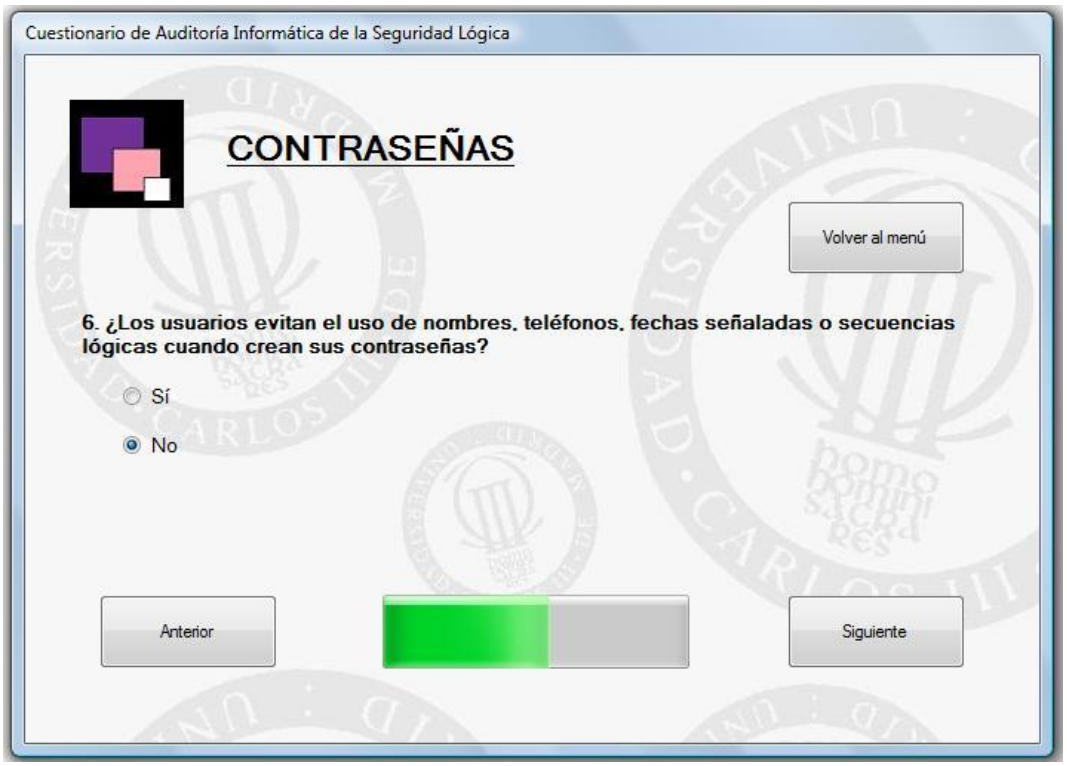


Figura 5.13 Contraseñas 7

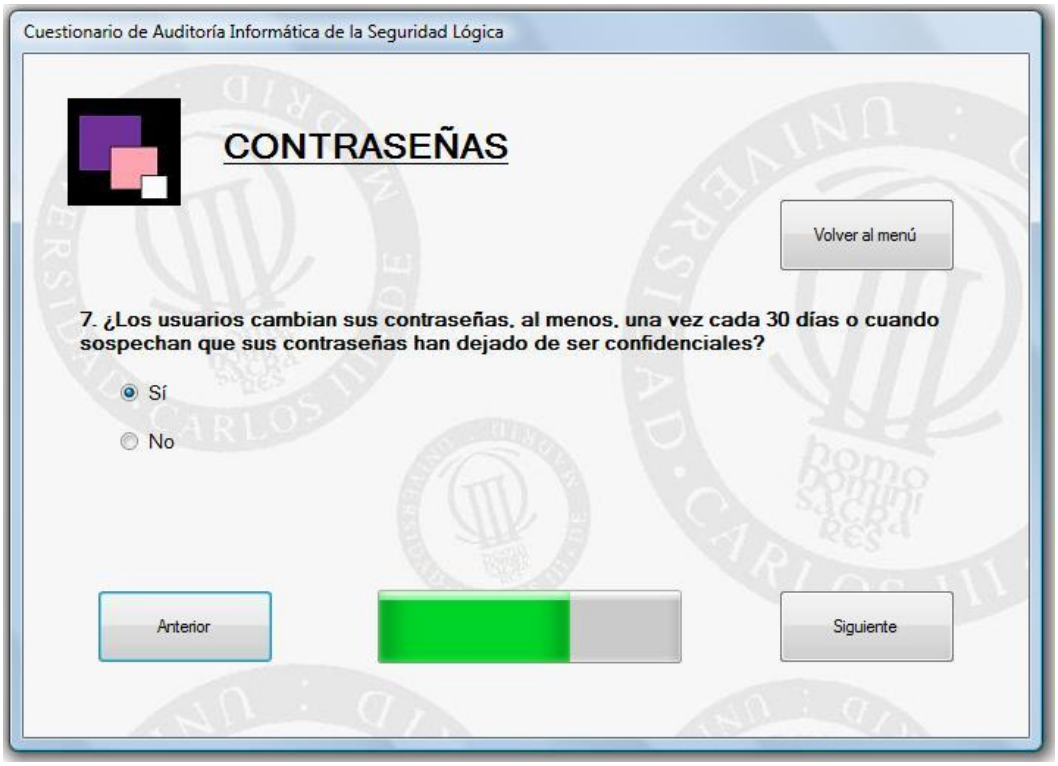


Figura 5.14 Contraseñas 8

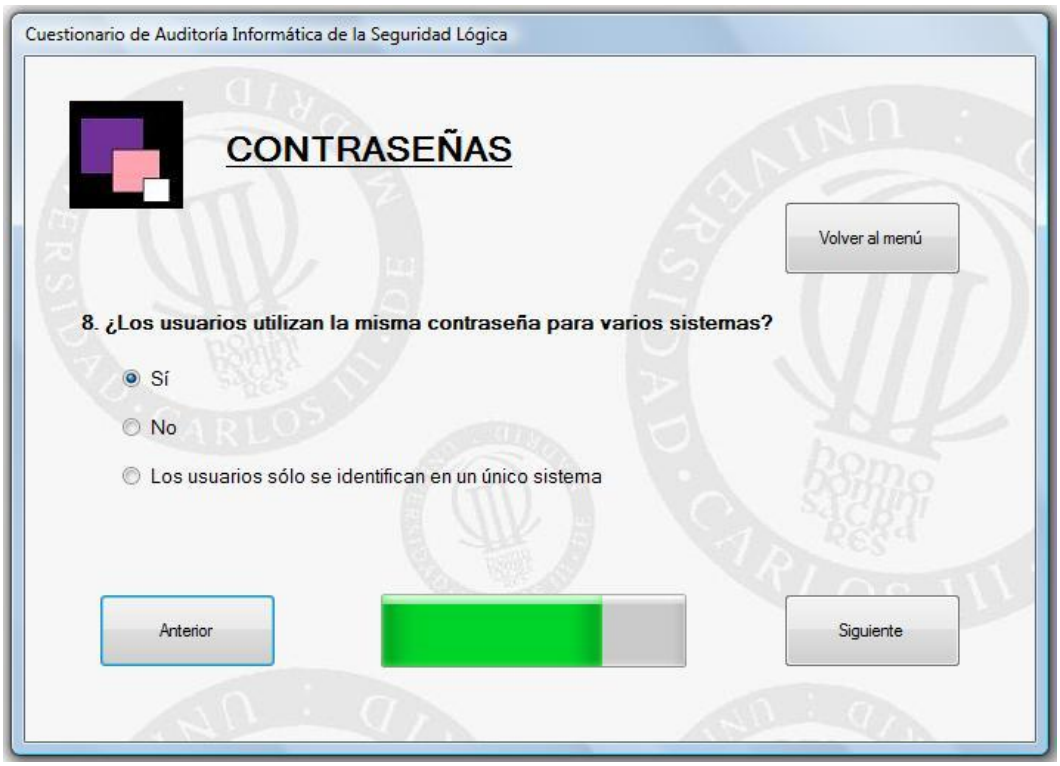


Figura 5.15 Contraseñas 9

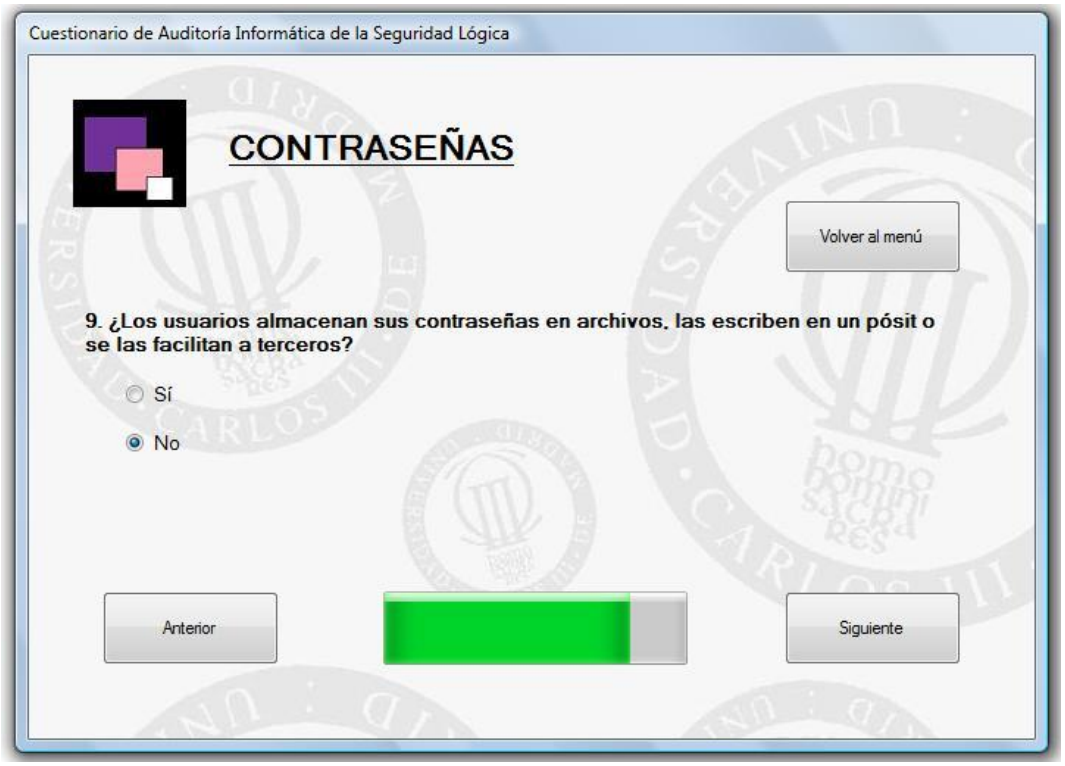


Figura 5.16 Contraseñas 10

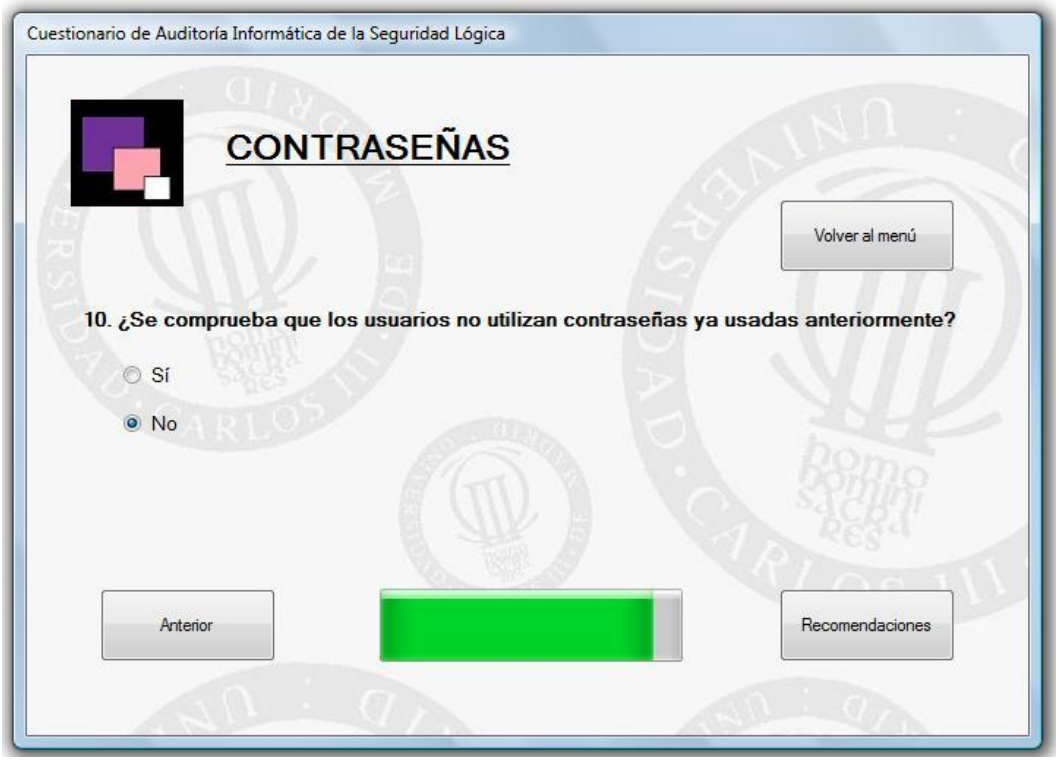
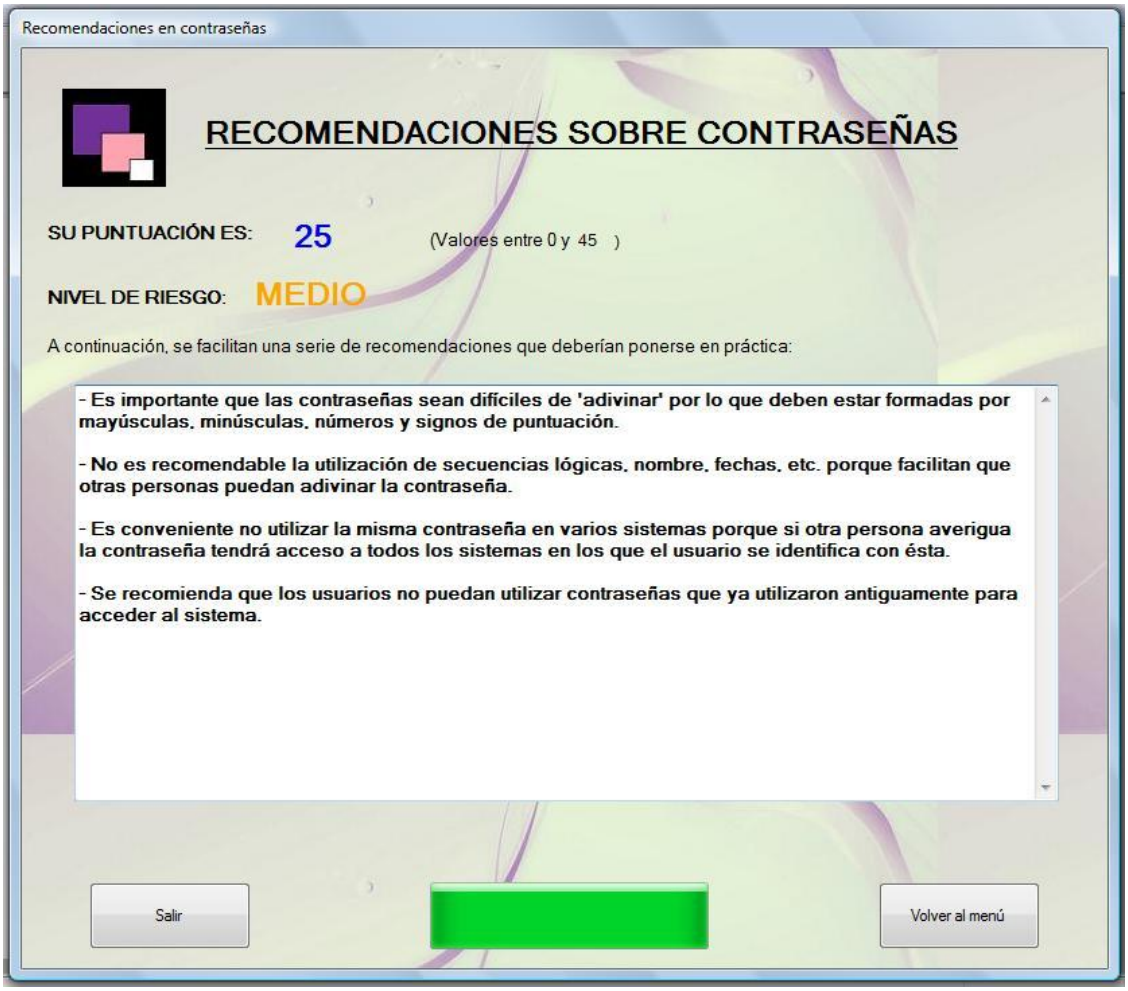


Figura 5.17 Contraseñas Recomendaciones



5. 4. 2 Caso práctico: Datos personales

La empresa "Y" maneja ficheros automatizados con datos de carácter personal desde 1994. La entidad no realiza transferencias internacionales de dichos datos y, en principio, no tiene intención de hacerlo.

Para proteger los datos personales conforme a la ley, la compañía se regía por la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD). Cuando se aprobó la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) se derogó la ley anterior y la organización tuvo que ponerse manos a la obra para adaptarse a la nueva ley.

En 2007, se publicó el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprobaba el Reglamento de desarrollo de la LOPD y la entidad se adaptó nuevamente a las exigencias del reglamento.

Todos los ficheros que contienen datos personales están notificados a la Agencia Española de Protección de Datos. Además, a dichos ficheros se les aplica al menos un nivel básico de seguridad. El responsable de los ficheros se encarga de adoptar las medidas necesarias para garantizar la seguridad de los datos personales.

Los derechos ARCO (acceso, rectificación, cancelación y oposición) se hacen efectivos en los plazos y las formas que indica la LOPD. Las personas de las que se recaban los datos personales dan su consentimiento inequívoco para el tratamiento de sus datos personales.

La entidad siempre informa a las personas de las que se recaban datos de carácter personal de la finalidad del fichero y destinatarios, de los datos que son obligatorios y opcionales, las consecuencias de facilitar los datos o no hacerlo y de informar de los derechos que tienen dichas personas.

Además, el responsable del fichero ha elaborado un documento de seguridad que recoge las medidas de índole técnica y organizativa aunque todavía no muestra una estructura clara y se encuentra en revisión para reelaborarlo conforme a la ley.

La compañía pretende comprobar hasta qué punto cumple la legislación vigente y qué debe mejorar para proteger los datos personales conforme a la ley. A continuación, se muestra las respuestas que han cumplimentado y las recomendaciones que debería llevar a la práctica:

Figura 5.18 Datos Personales 1

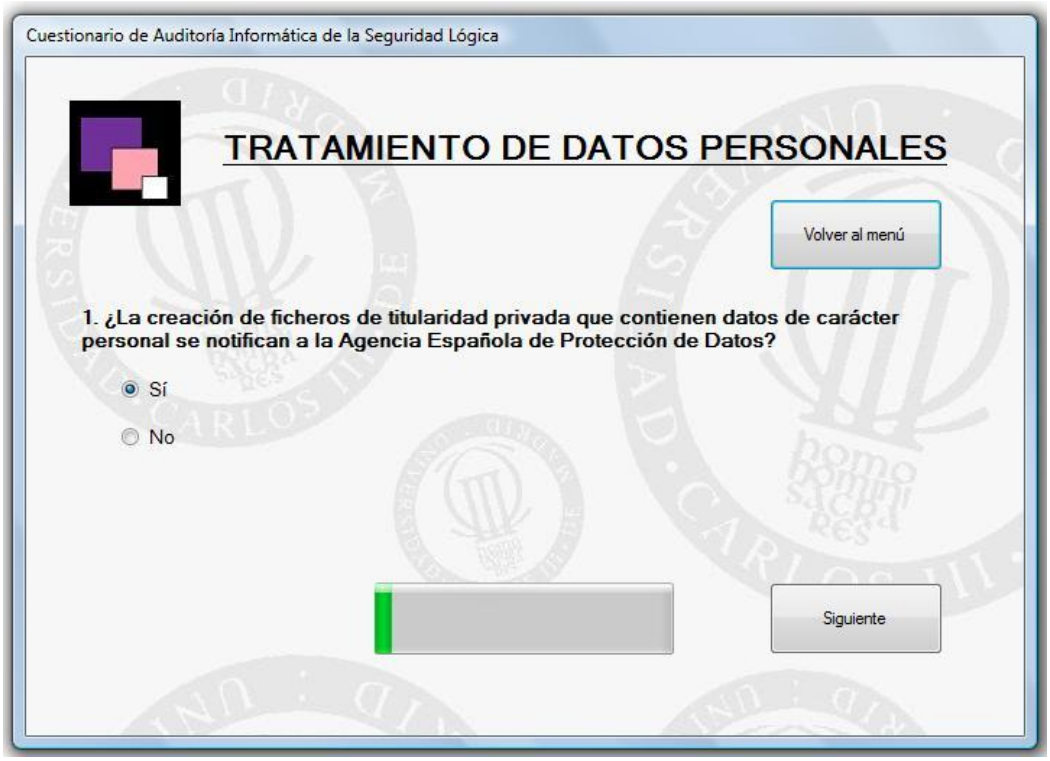


Figura 5.19 Datos Personales 2

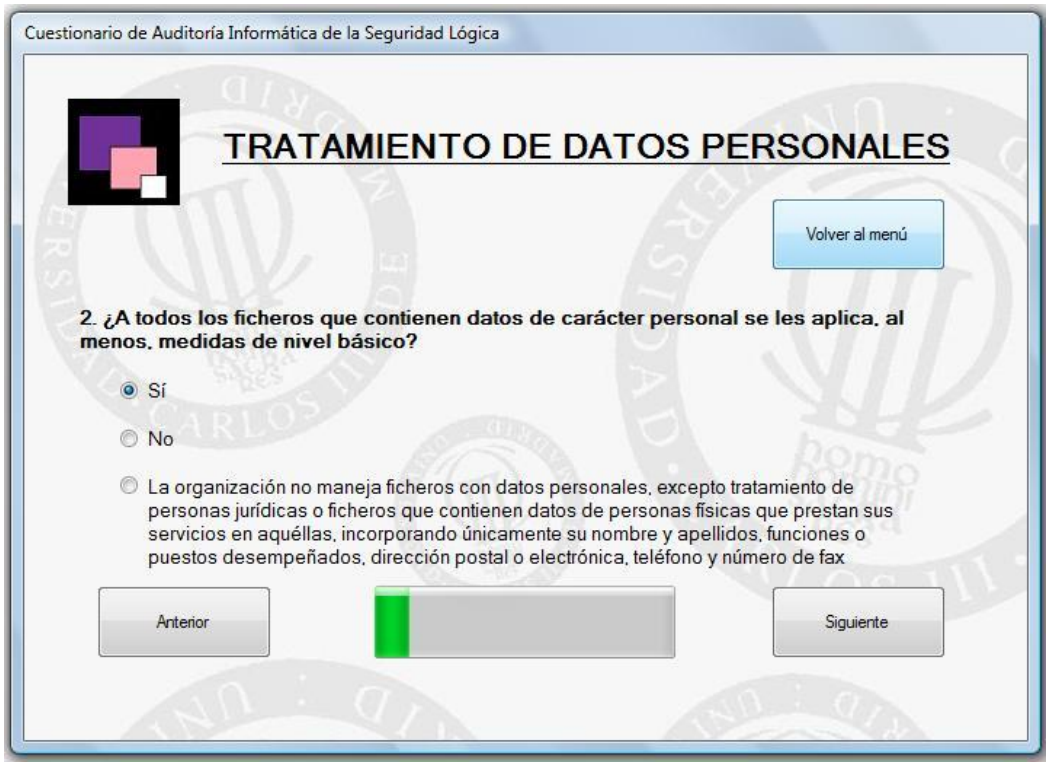


Figura 5.20 Datos Personales 3

Figura 5.21 Datos Personales 4

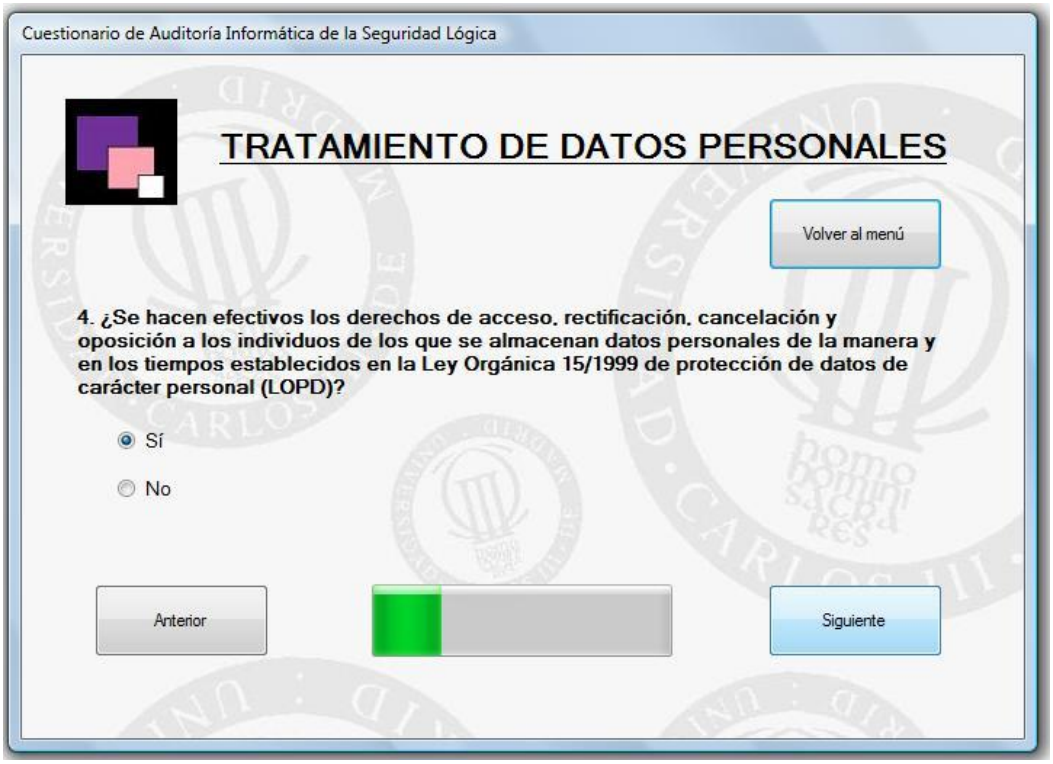


Figura 5.22 Datos Personales 5

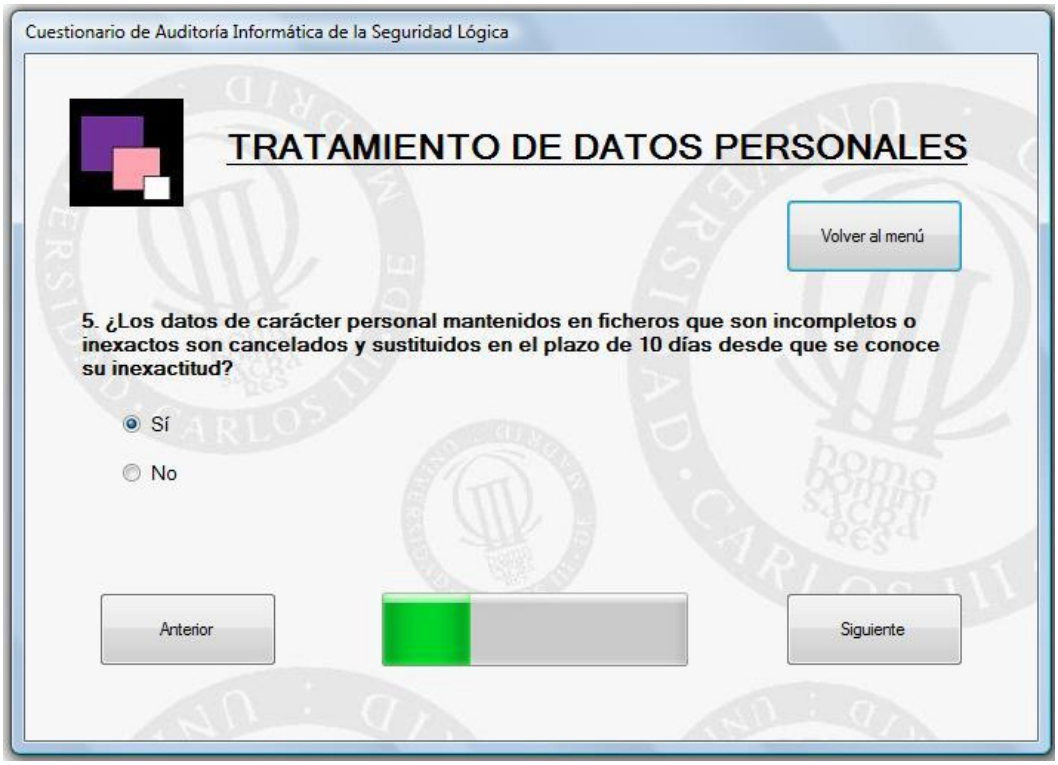


Figura 5.23 Datos Personales 6

Figura 5.24 Datos Personales 7

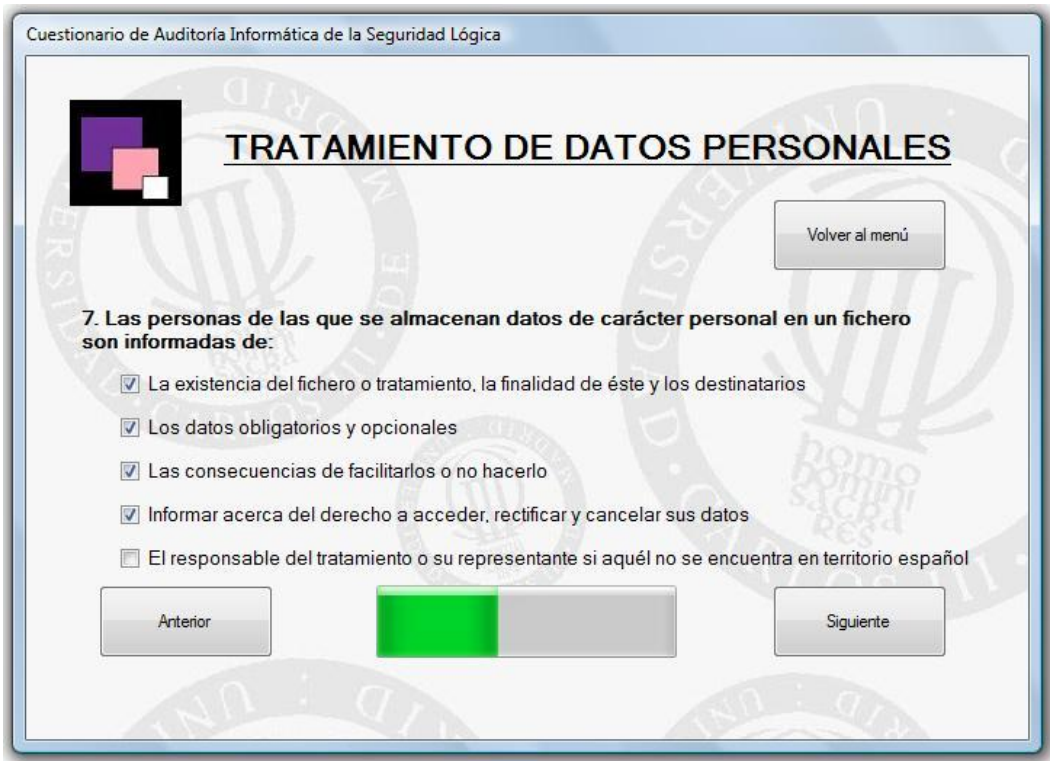


Figura 5.25 Datos Personales 8

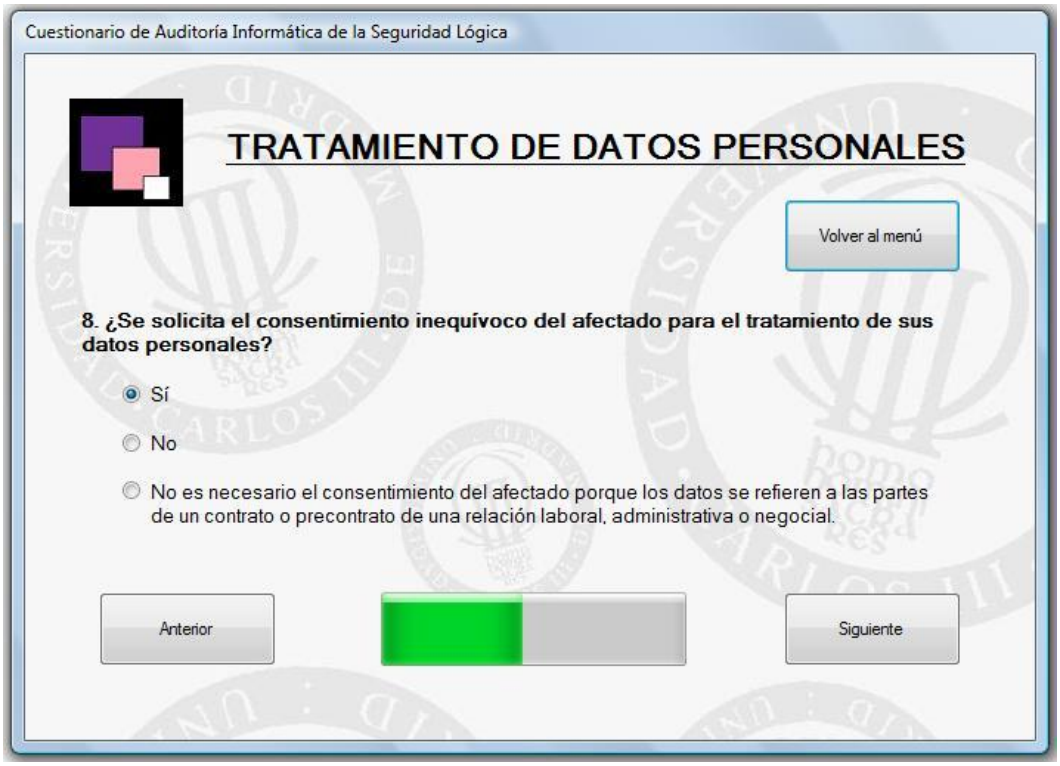


Figura 5.26 Datos Personales 9

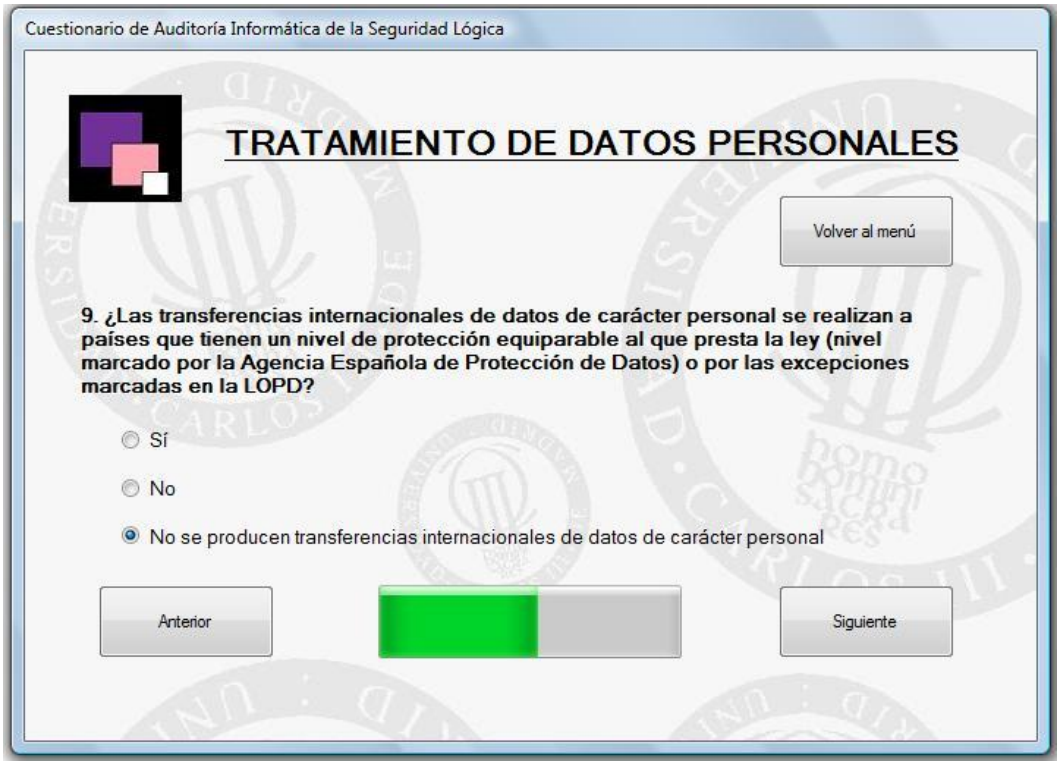


Figura 5.27 Datos Personales 10

Figura 5.28 Datos Personales 11

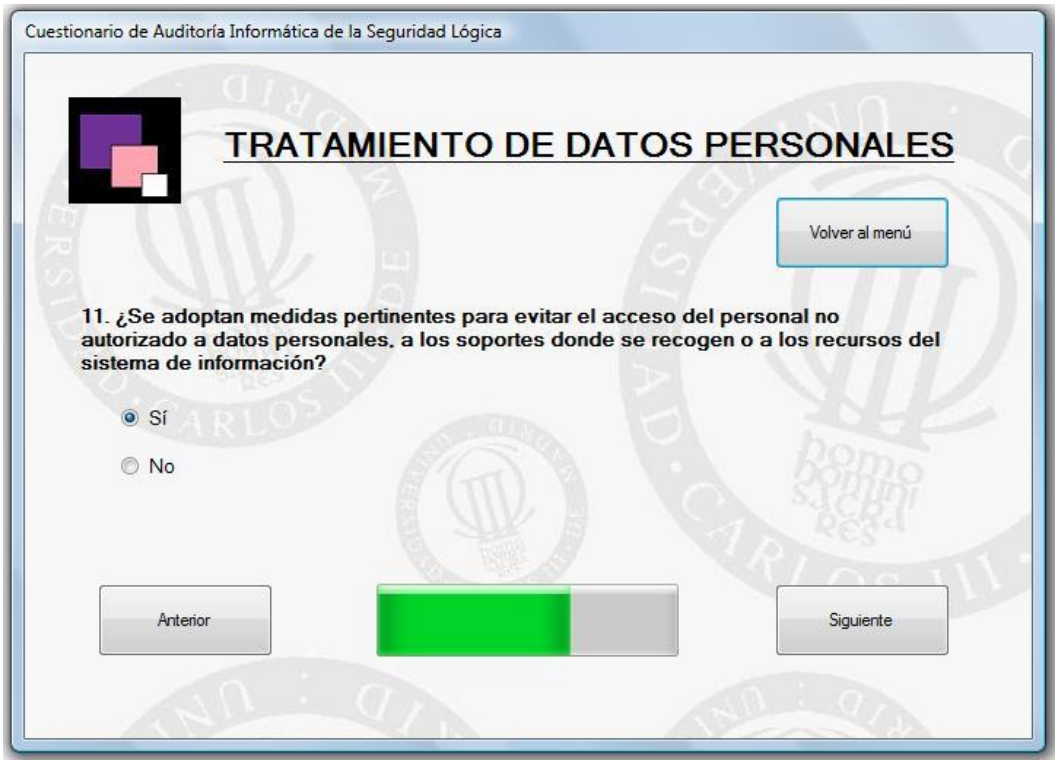


Figura 5.29 Datos Personales 12

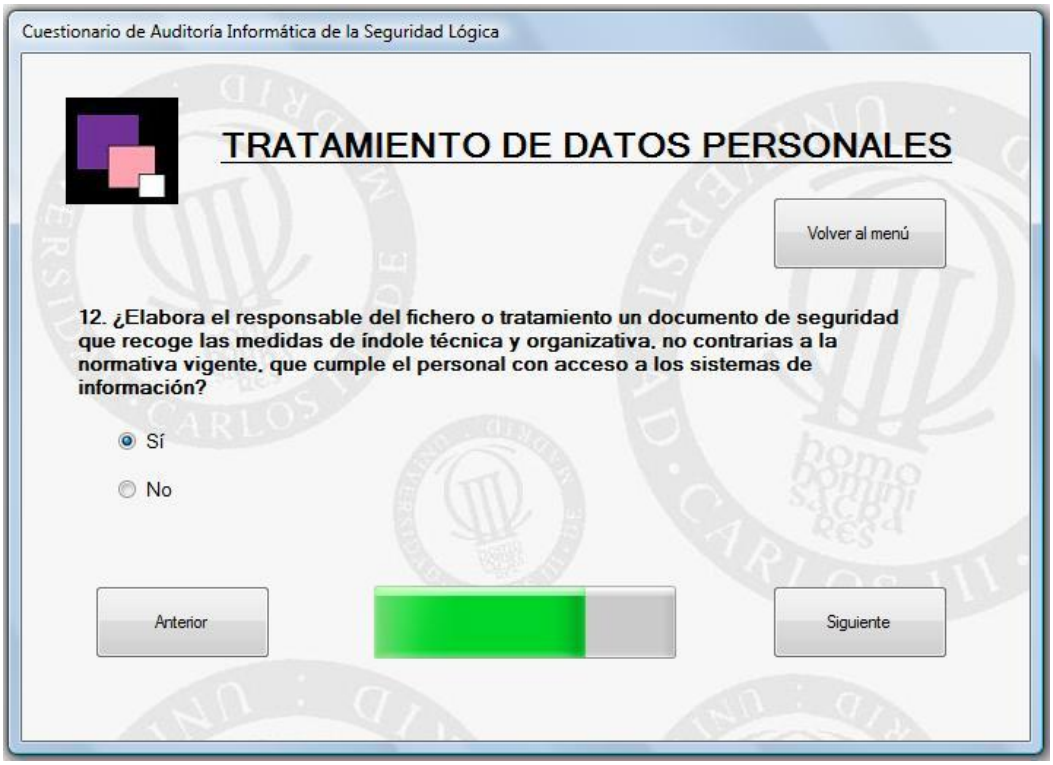


Figura 5.30 Datos Personales 13

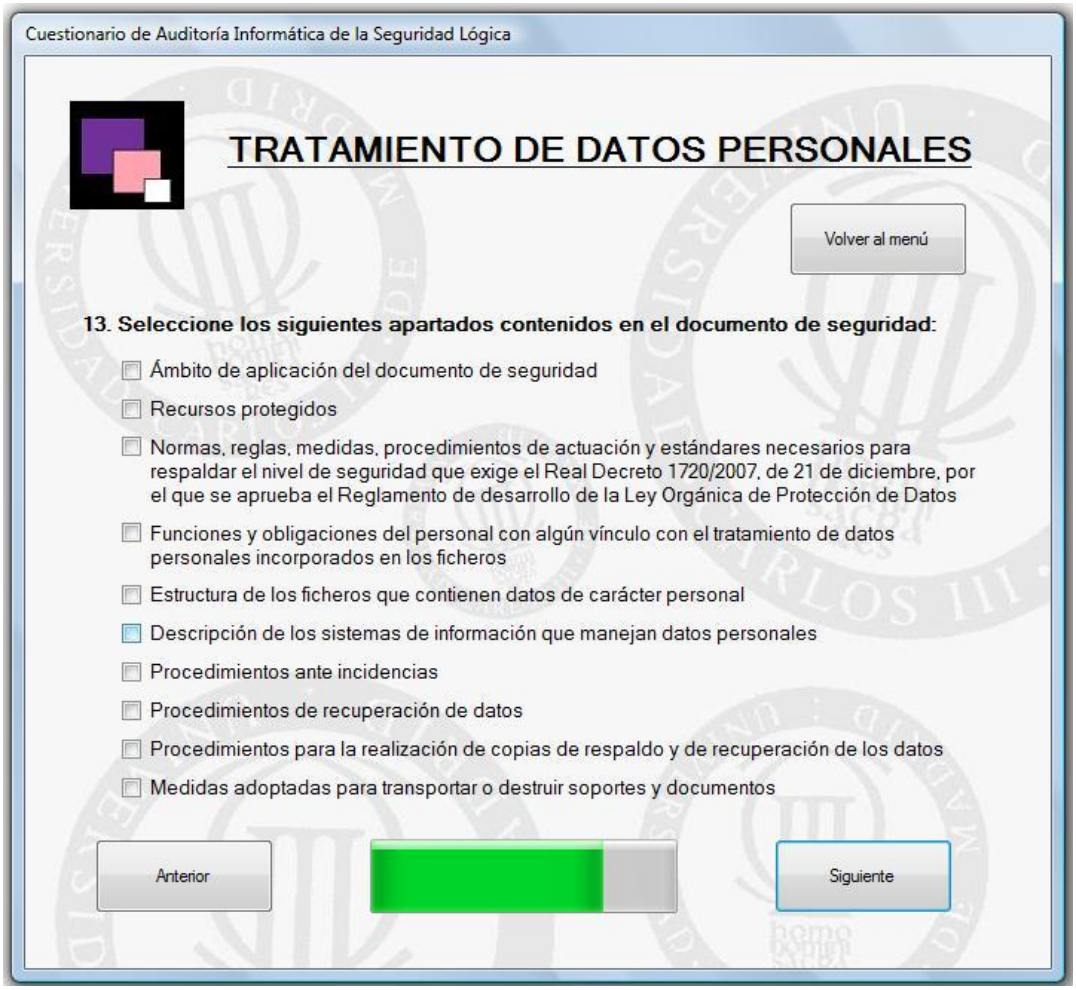


Figura 5.31 Datos Personales 14

Figura 5.32 Datos Personales 15

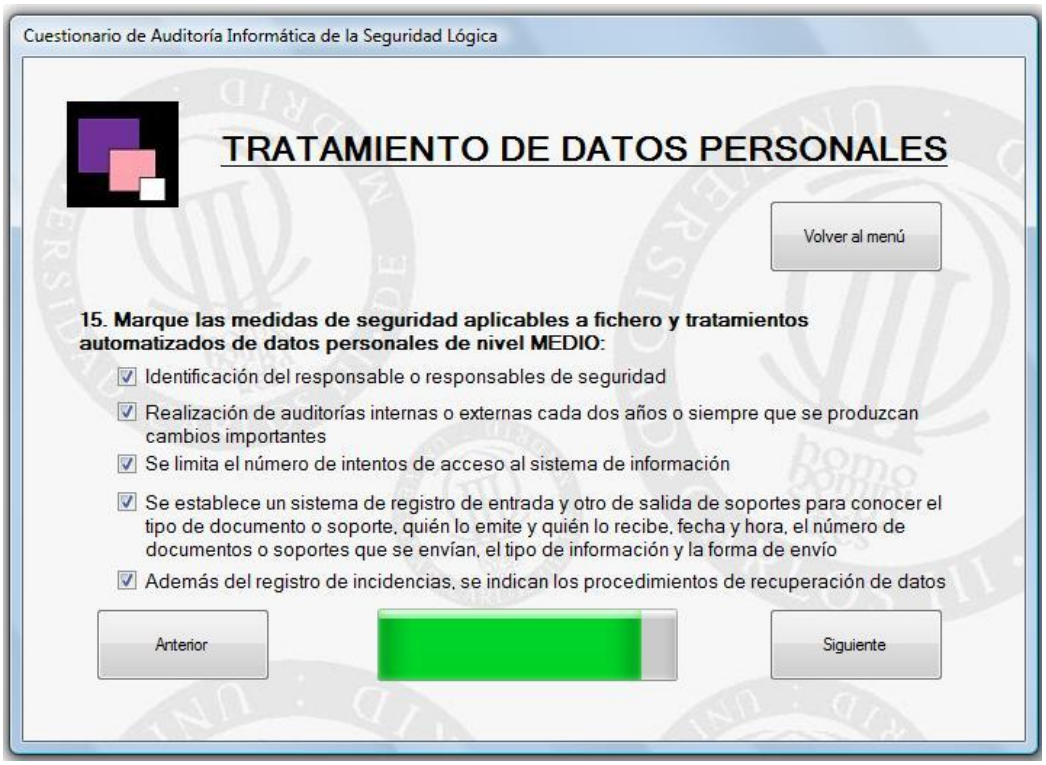


Figura 5.33 Datos Personales 16

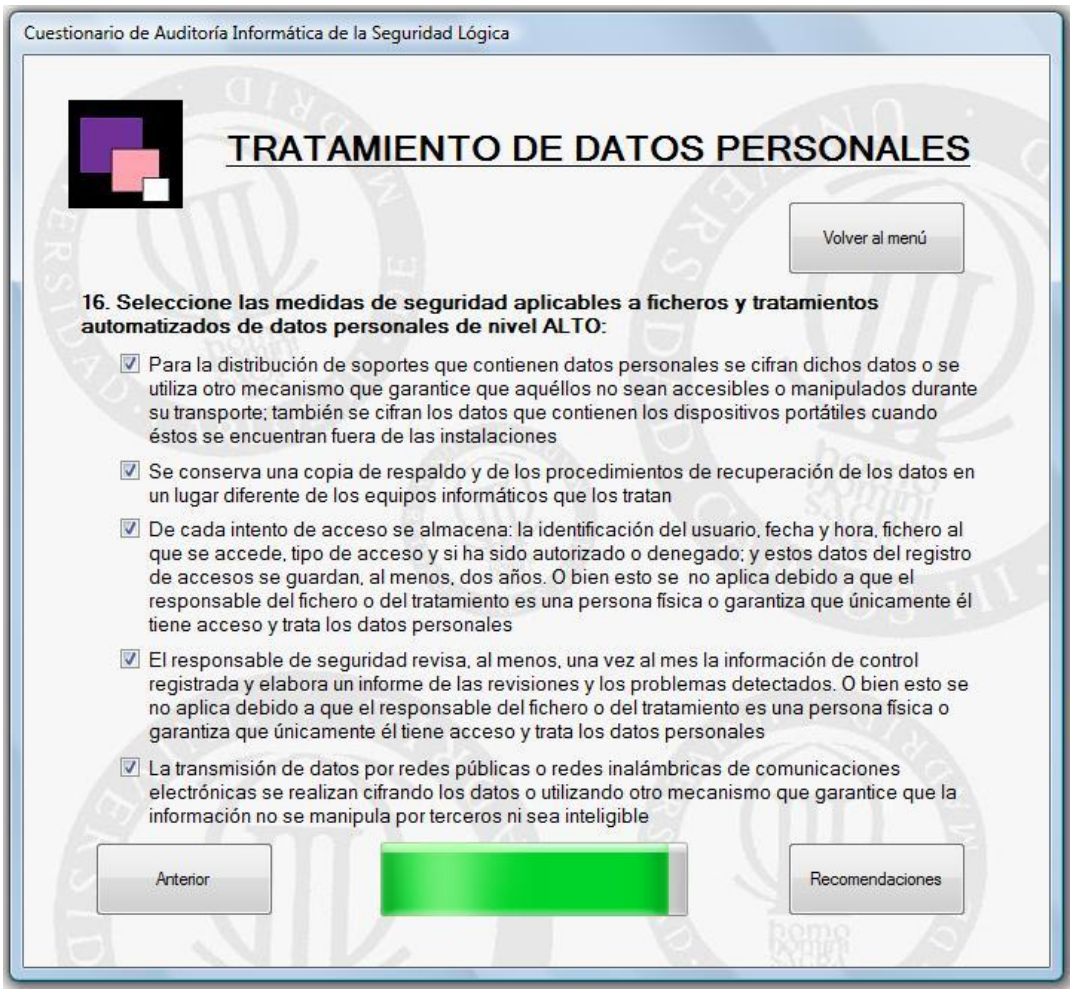
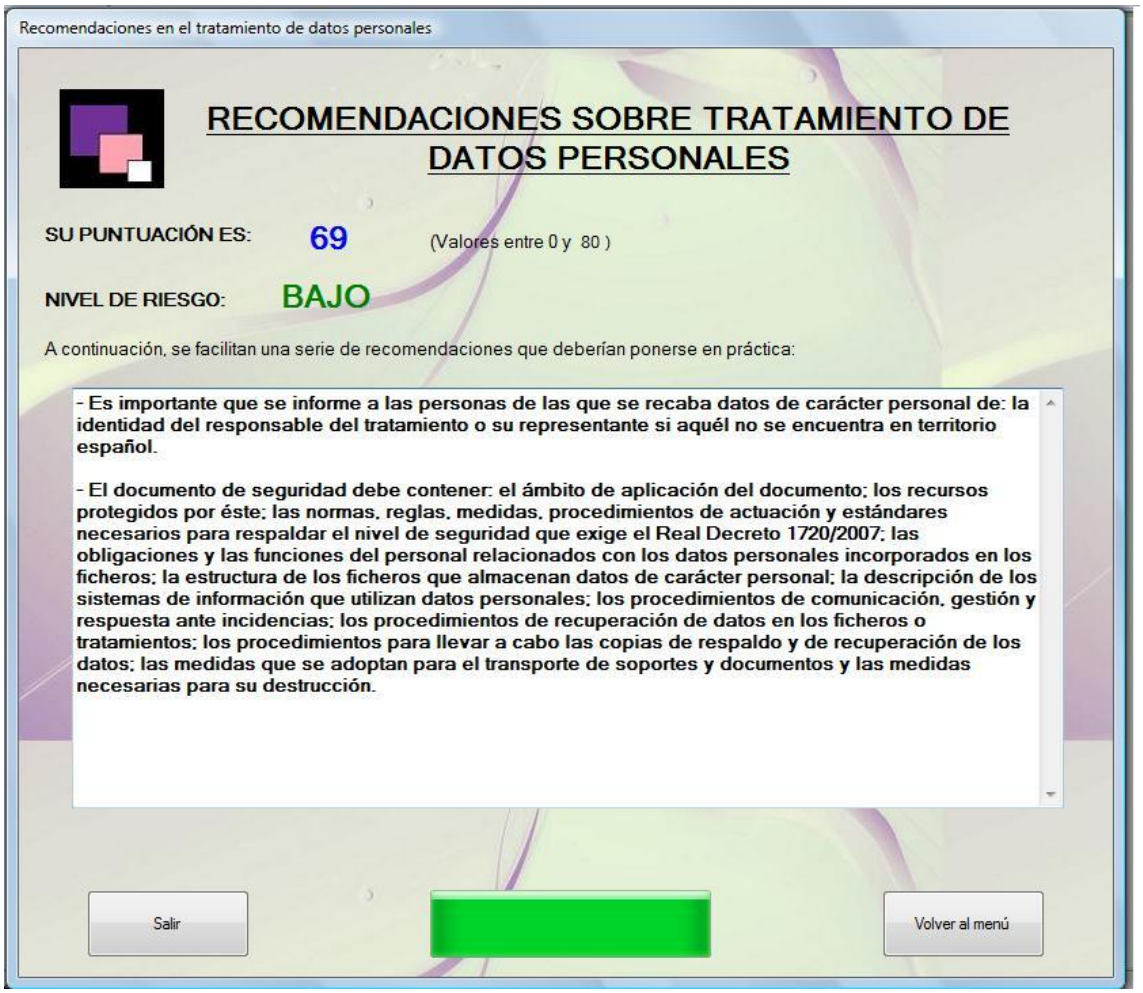


Figura 5.34 Datos Personales Recomendaciones



5. 4. 3 Caso práctico: Control de acceso lógico

La compañía "Z" se propone implantar controles de acceso lógico a su sistema de información para restringir el acceso a la información confidencial. Se dispone a completar el apartado de "*Control de acceso lógico*".

Figura 5.35 Control de acceso lógico 1

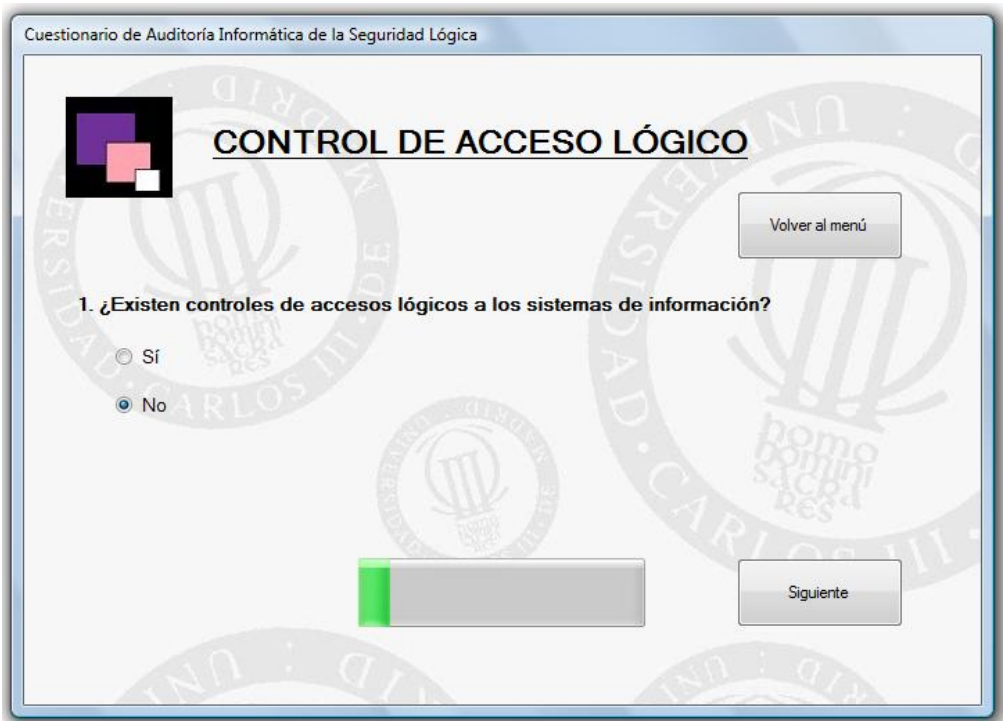
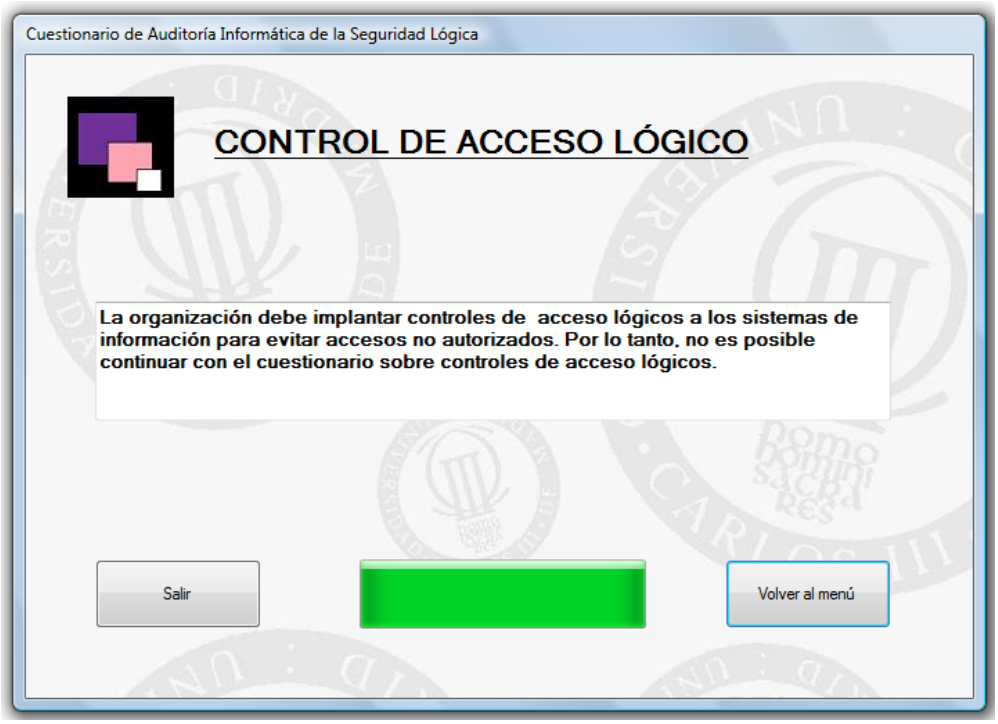


Figura 5.36 Control de acceso lógico Advertencia



5. 4. 4 Caso práctico: Control de acceso lógico (II)

La entidad "A" tiene contratadas a 90 personas para trabajar con su sistema de información. Hace dos años, implantó controles de acceso lógico para evitar que personas no autorizadas accedieran al sistema.

La compañía no creyó necesario formar a los empleados en la utilización de dichos controles porque no requerían altos conocimientos para su uso. Cada tres meses, se revisan los controles para cerciorarse de que cumplen su cometido y se encuentran en perfecto estado.

Sin embargo, no se limita el número de intentos de acceso al sistema por lo que un intruso podría intentar acceder de forma reiterada a éste. Tampoco se mantiene una lista actualizada con las personas que tienen acceso autorizado ni se registran en *logs*, los accesos al sistema: en qué fecha y hora, qué persona… ya sean accesos acreditados o ilícitos.

En cambio, cuando un empleado es despedido inmediatamente se le revoca el derecho de acceso al sistema para que no pueda causar ningún daño. Los usuarios tienen acceso a todo el sistema aunque tienen perfectamente definidas sus funciones y saben que aplicaciones necesitan para desempeñar su trabajo.

El auditor utiliza toda esta información recabada por medio de entrevistas y cuestionarios para introducirla en la aplicación y obtener las recomendaciones que reflejará en el informe final.

Figura 5.37 Control de acceso lógico (II) 1

Figura 5.38 Control de acceso lógico (II) 2

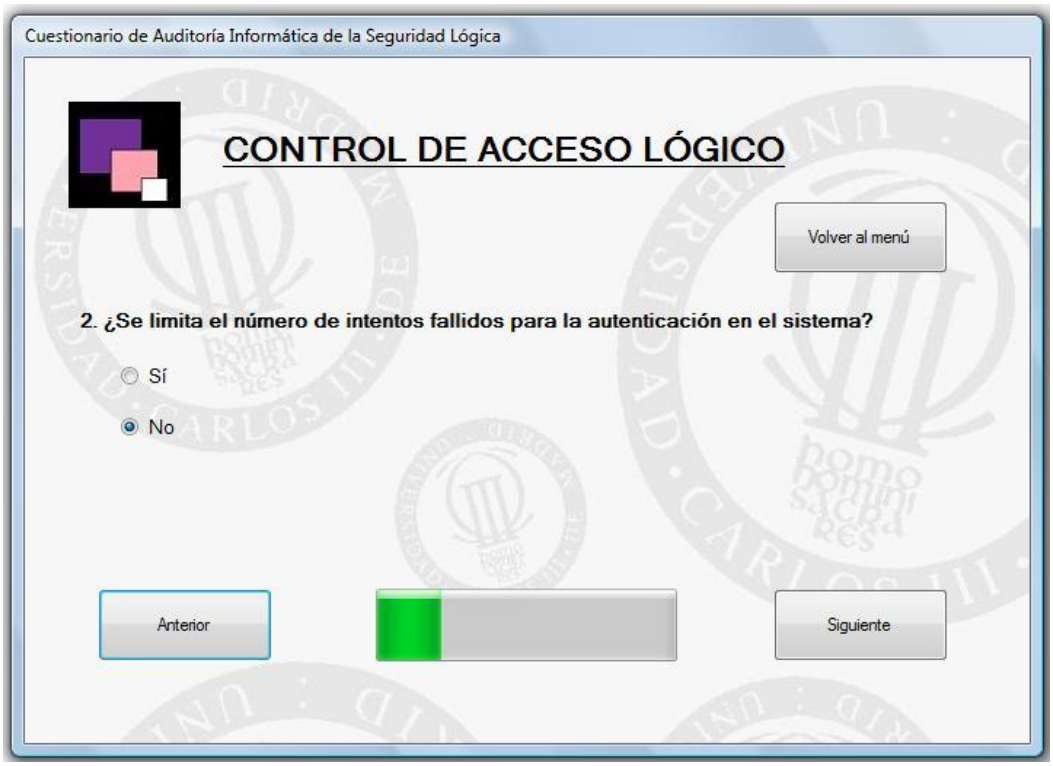


Figura 5.39 Control de acceso lógico (II) 3

Figura 5.40 Control de acceso lógico (II) 4

Figura 5.41 Control de acceso lógico (II) 5

Figura 5.42 Control de acceso lógico (II) 6

Figura 5.43 Control de acceso lógico (II) 7

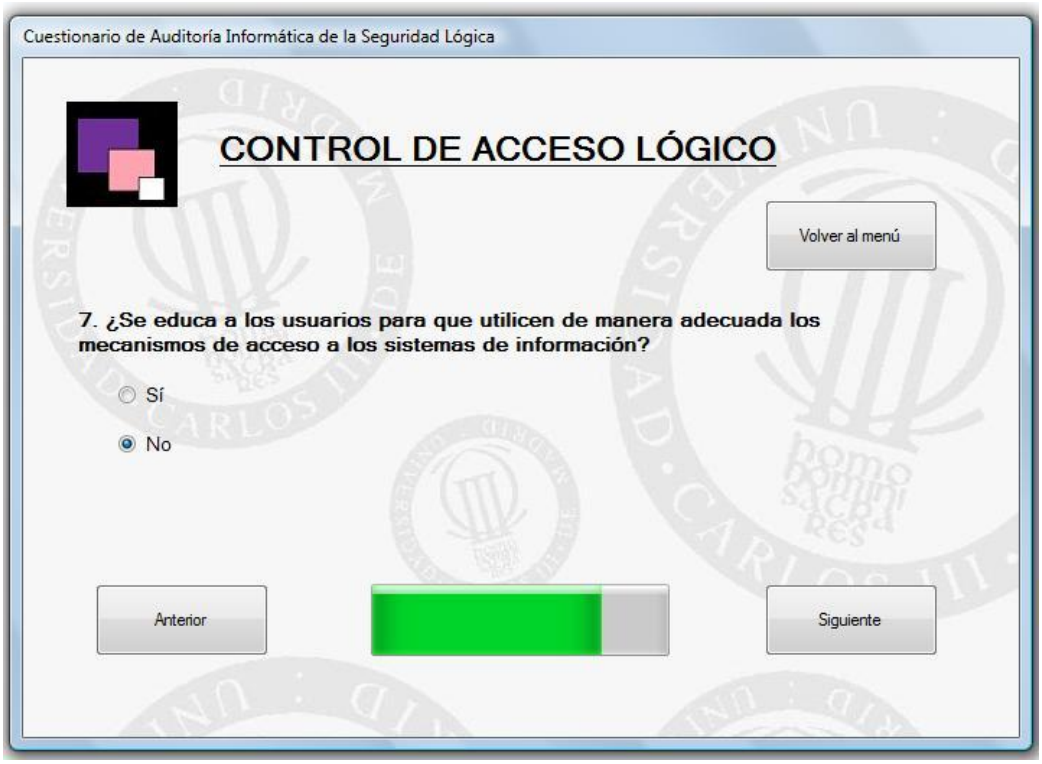
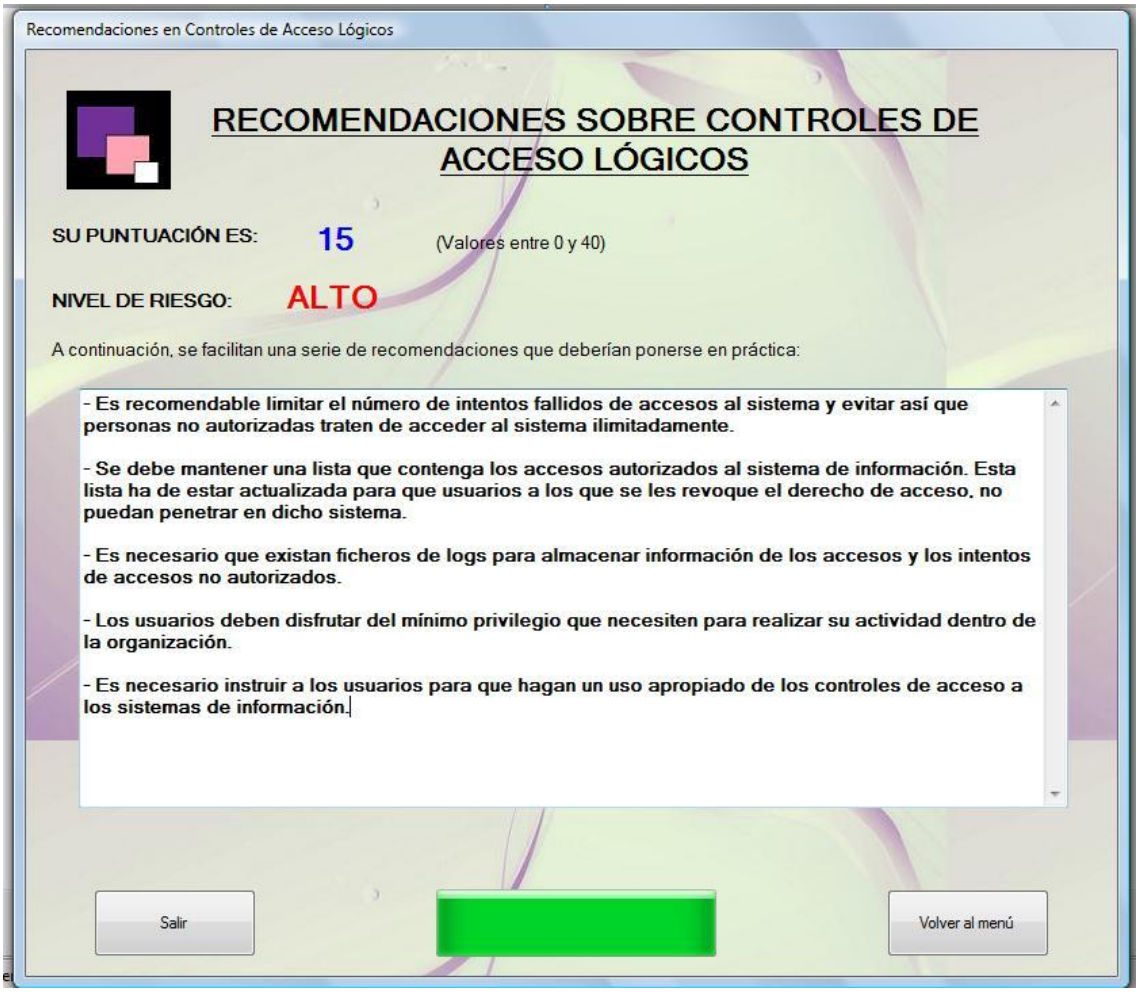


Figura 5.44 Control de acceso lógico (II) 8

Figura 5.45 Control de acceso lógico (II) Recomendaciones



5. 4. 5 Caso práctico: Política de seguridad (I)

La empresa "B" cuenta con una política de la empresa que refleja las normas y reglas que impone la dirección a sus empleados. Esta política es revisada periódicamente y difundida entre los trabajadores para su comprensión y aceptación.

Sin embargo, no se ha definido todavía una política de seguridad que podría incluirse en el documento que contiene la política de la entidad o en otro. Por lo tanto, no se puede completar el apartado de "*Política de seguridad*".

Figura 5.46 Política de seguridad 1

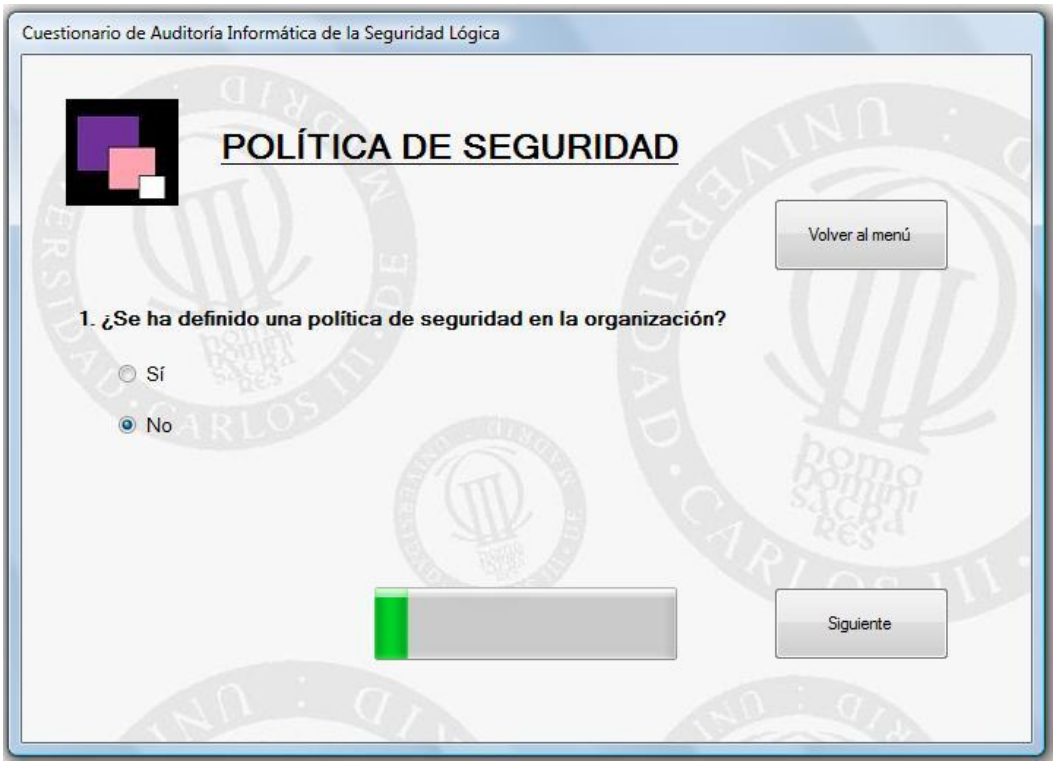
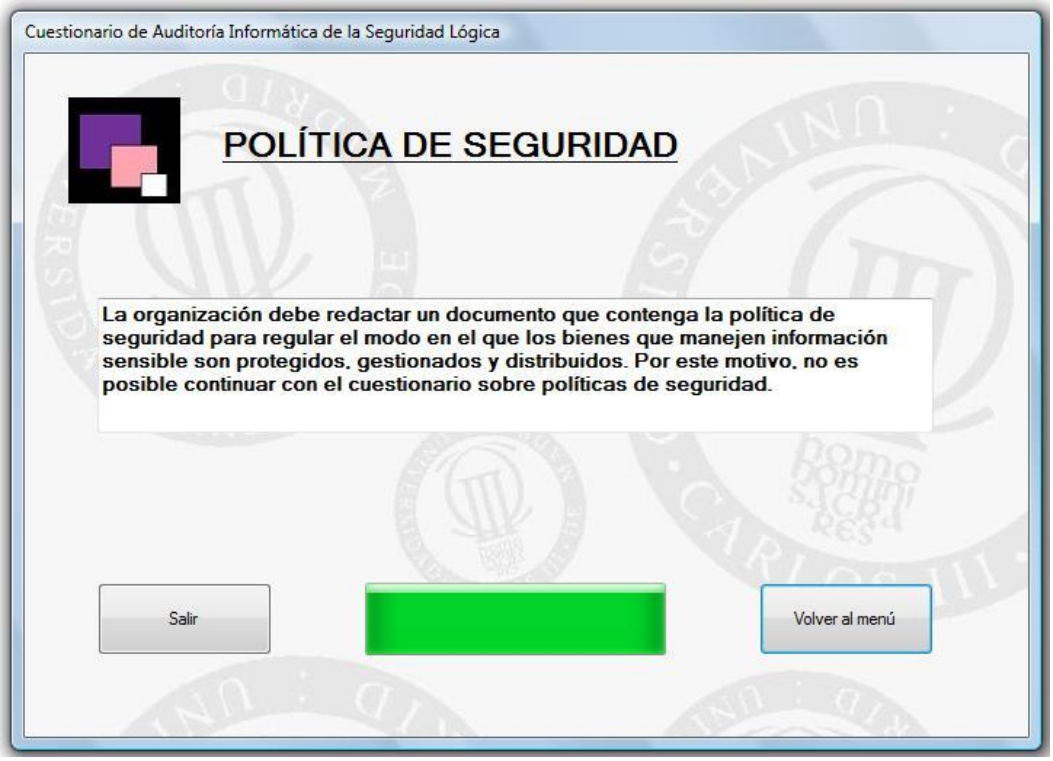


Figura 5.47 Política de seguridad Advertencia



5. 4. 6 Caso práctico: Política de seguridad (II)

En el año 2007, la organización "C" elaboró un documento que recogía la política de seguridad acorde a la política de la empresa. Esta política de seguridad fue escrita en un lenguaje sofisticado que contenía gran cantidad de tecnicismos entendibles por la alta dirección.

Desde entonces, no se ha revisado la política ni se ha adaptado a las nuevas normas legales ya que se ha ido posponiendo dicha revisión sin que finalmente, se haya llevado a cabo a día de hoy. Entre los planes de la compañía está designar un responsable de seguridad que inicie la revisión y modificación de la política.

Debido a que dicha política no está actualizada, no se fomenta su comunicación entre los empleados. Por este motivo y puesto que no está escrita en un lenguaje entendible por todo el personal de la empresa, no se cumple a todos los niveles.

Figura 5.48 Política de seguridad (II) 1

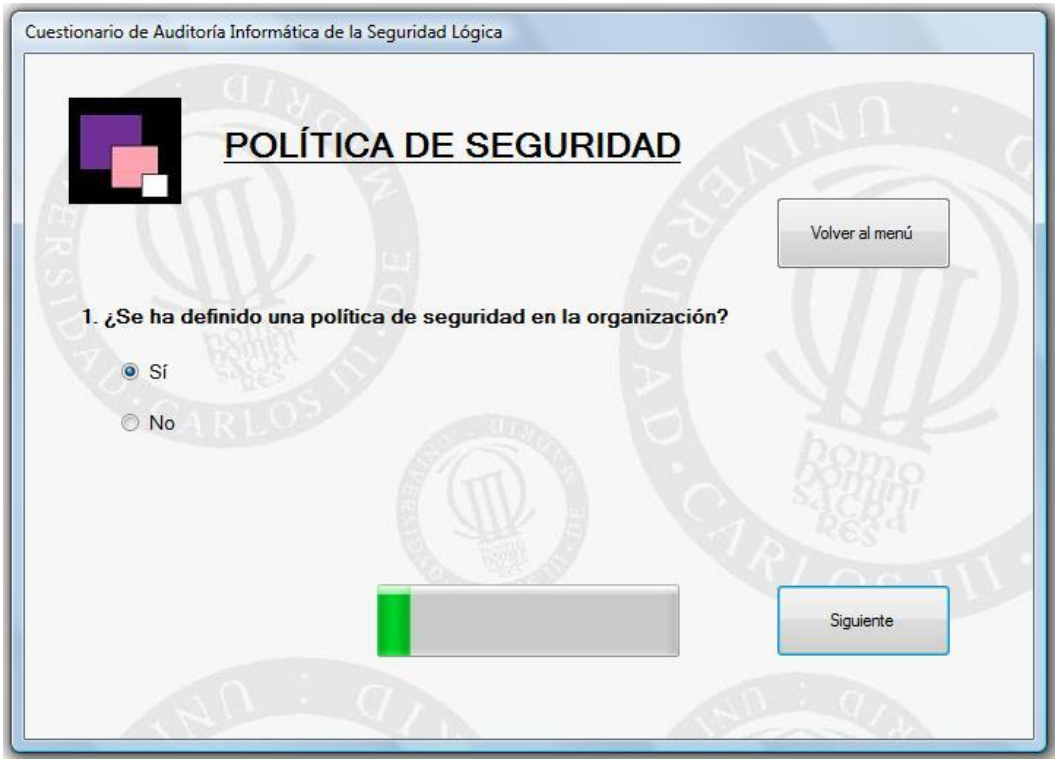


Figura 5.49 Política de seguridad (II) 2

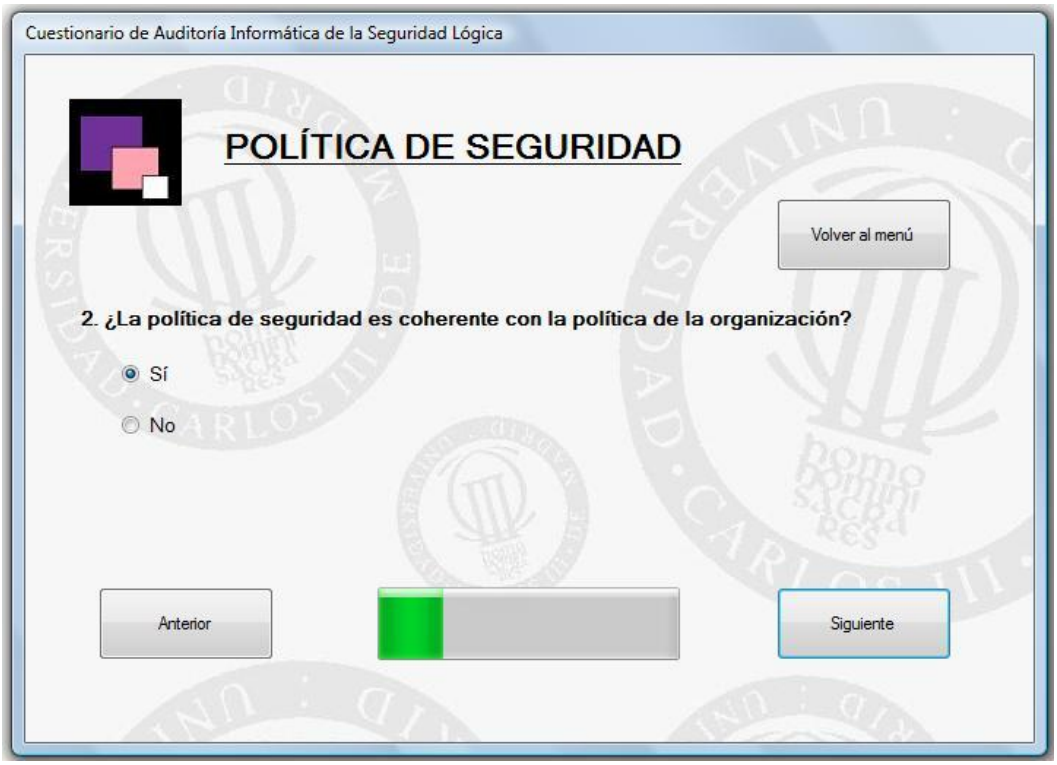


Figura 5.50 Política de seguridad (II) 3

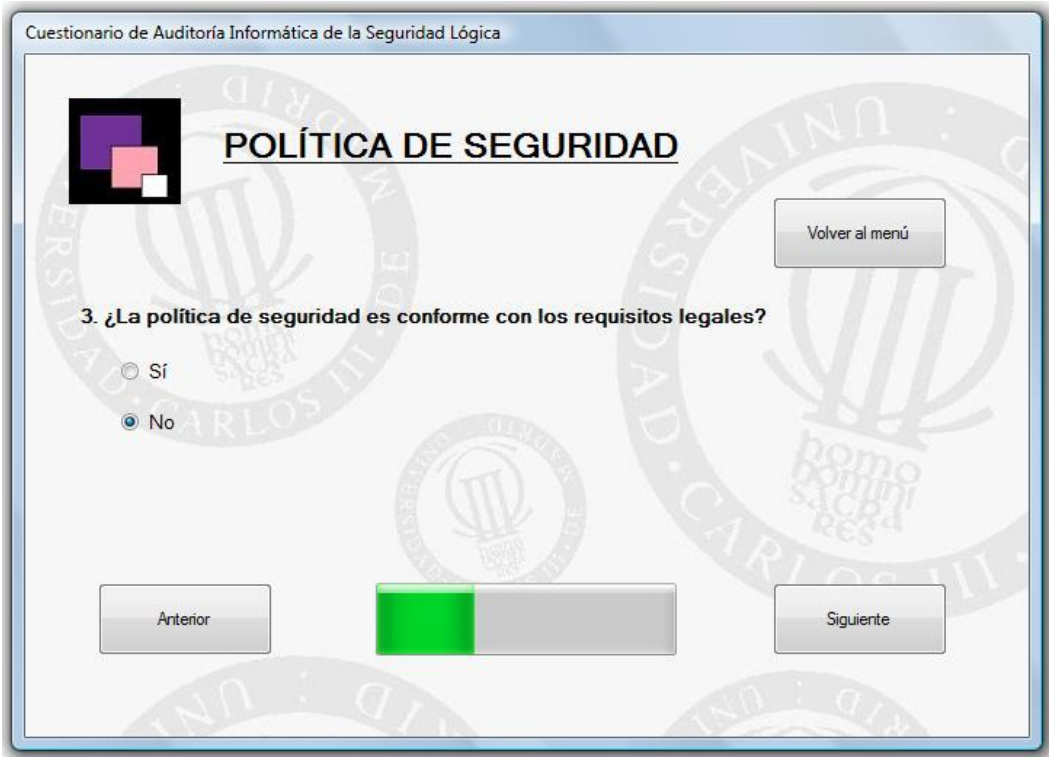


Figura 5.51 Política de seguridad (II) 4

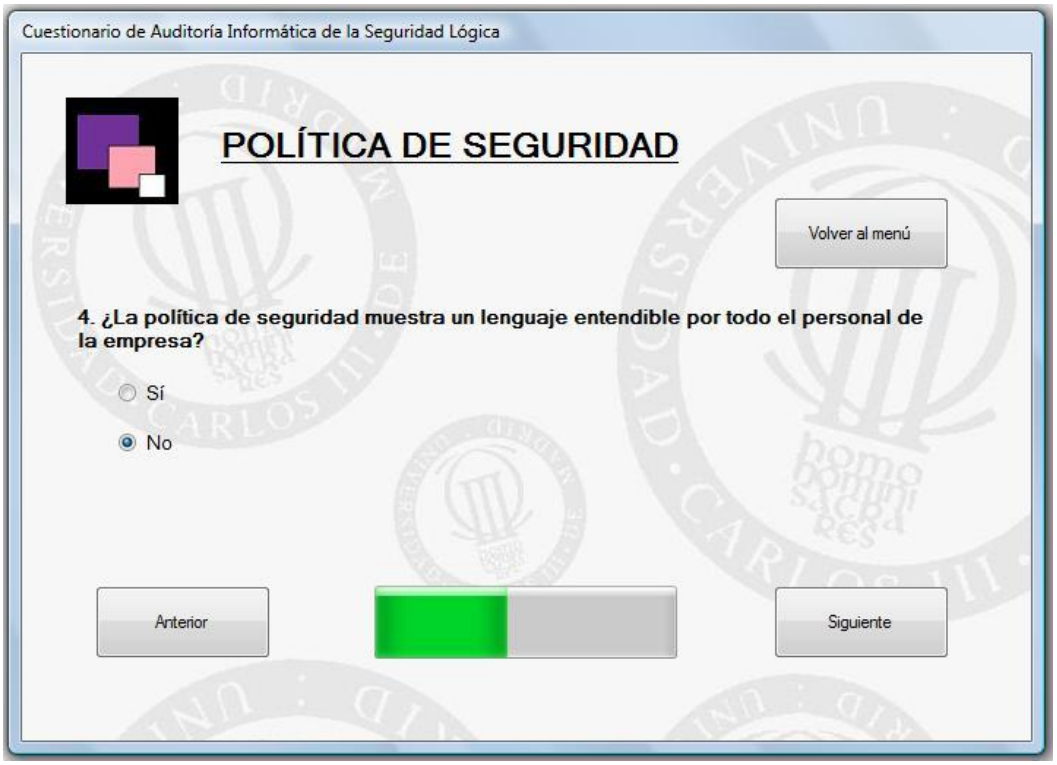


Figura 5.52 Política de seguridad (II) 5

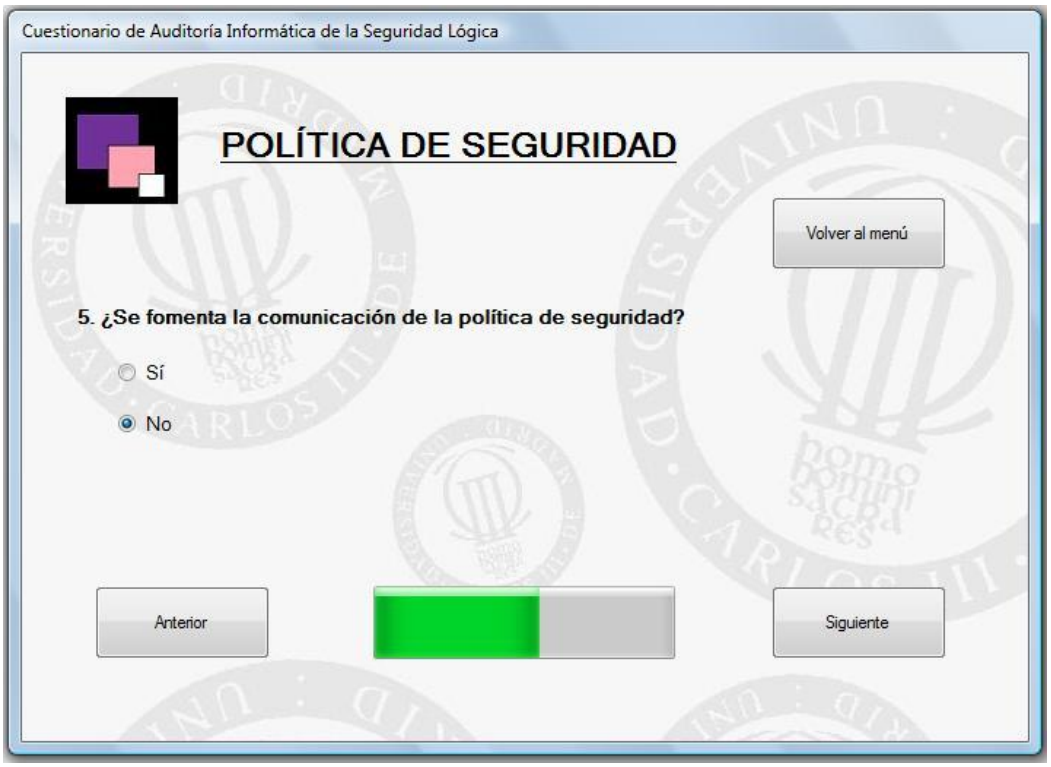


Figura 5.53 Política de seguridad (II) 6

Figura 5.54 Política de seguridad (II) 7

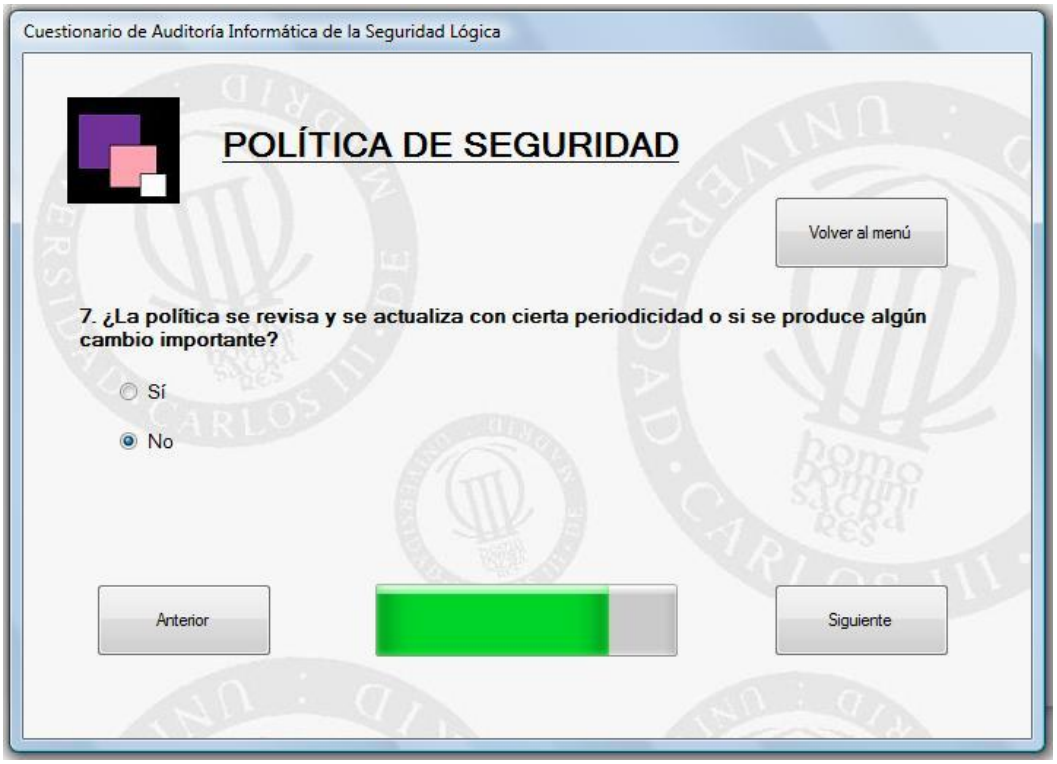


Figura 5.55 Política de seguridad (II) 8

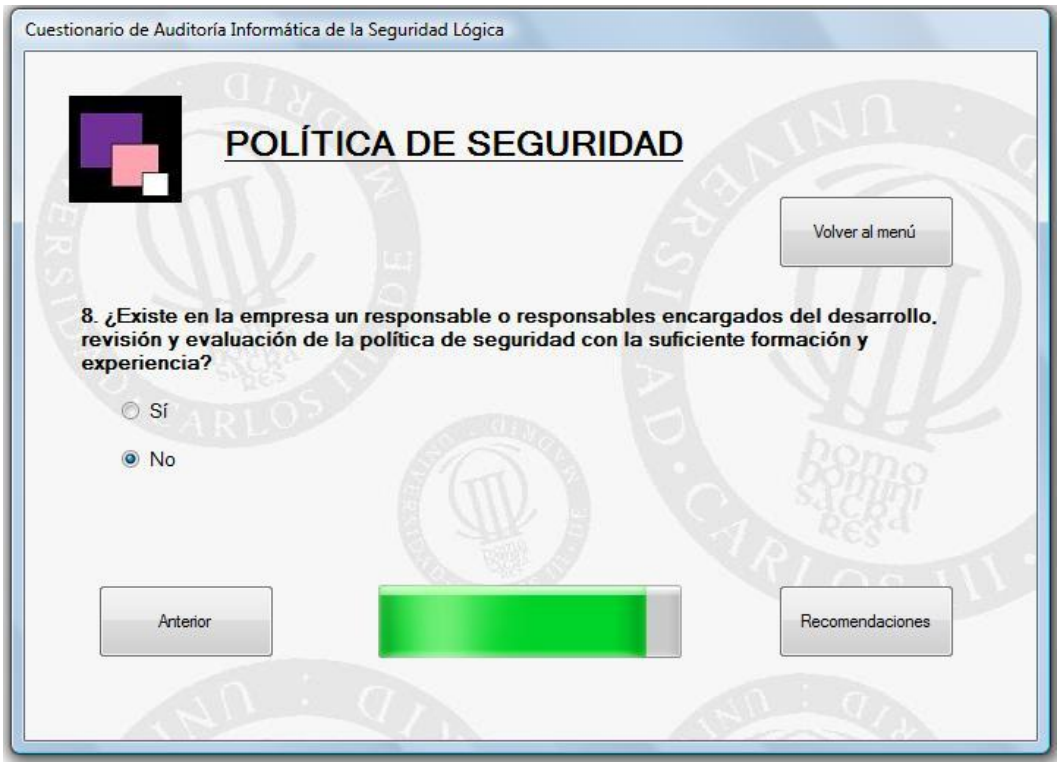
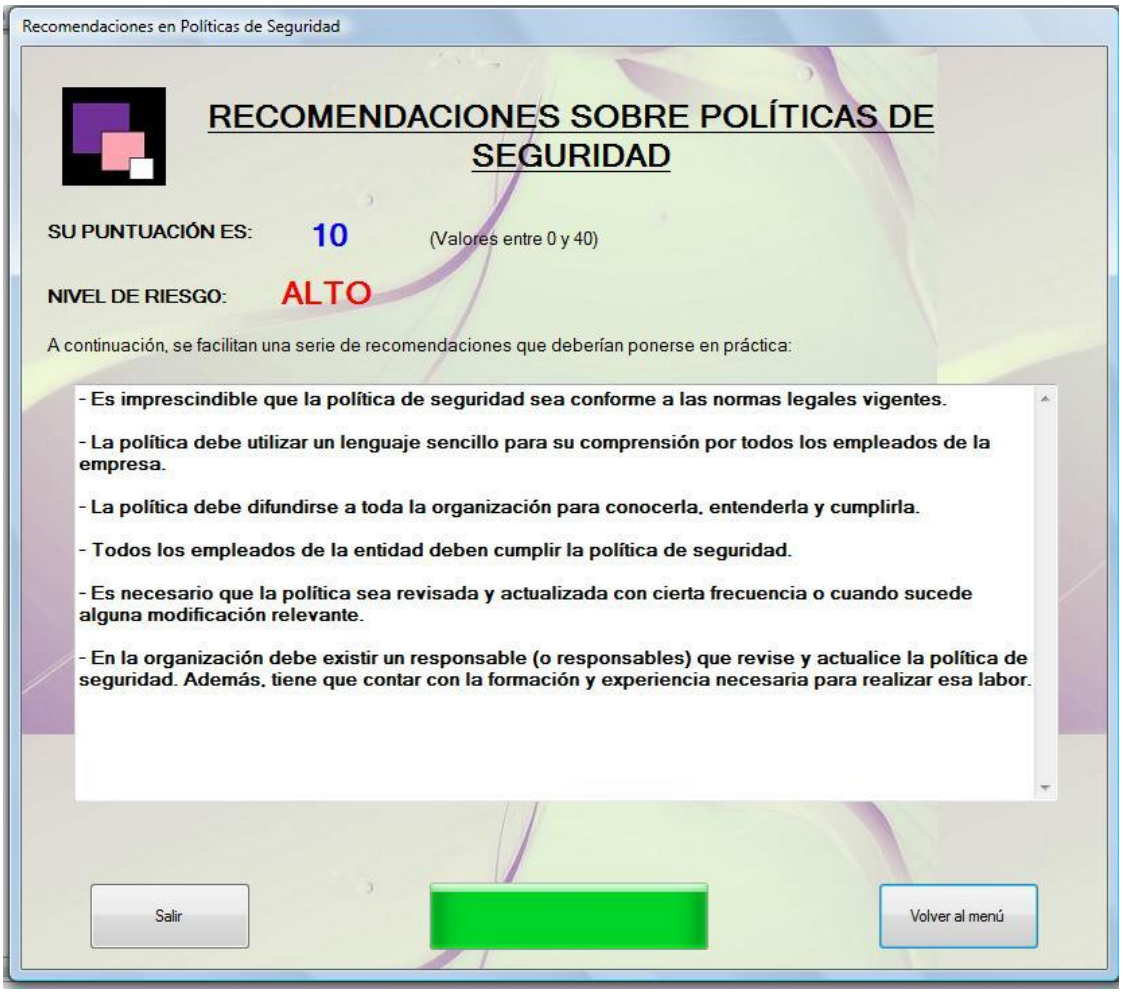


Figura 5.56 Política de seguridad (II) Recomendaciones



5. 4. 7 Caso práctico: Copias de seguridad (I)

En 2008, la empresa familiar "D" comenzó su actividad. Esta compañía maneja gran cantidad de datos de carácter personal de sus clientes en ficheros automatizados. Entre esos datos figuran datos de nivel medio. Cada dos años, al menos, debe someterse a una auditoría para comprobar que todo está en orden y se cumplen las medidas de seguridad que recoge el Real Decreto 1720/2007.

Este año, la compañía se va a someter a su primera auditoría. Sin embargo, los resultados no son muy favorables. El bloque de preguntas de "*Copias de seguridad*" no puede completarlo puesto que esta entidad no realiza respaldos de la información.

Figura 5.57 Copias de seguridad 1

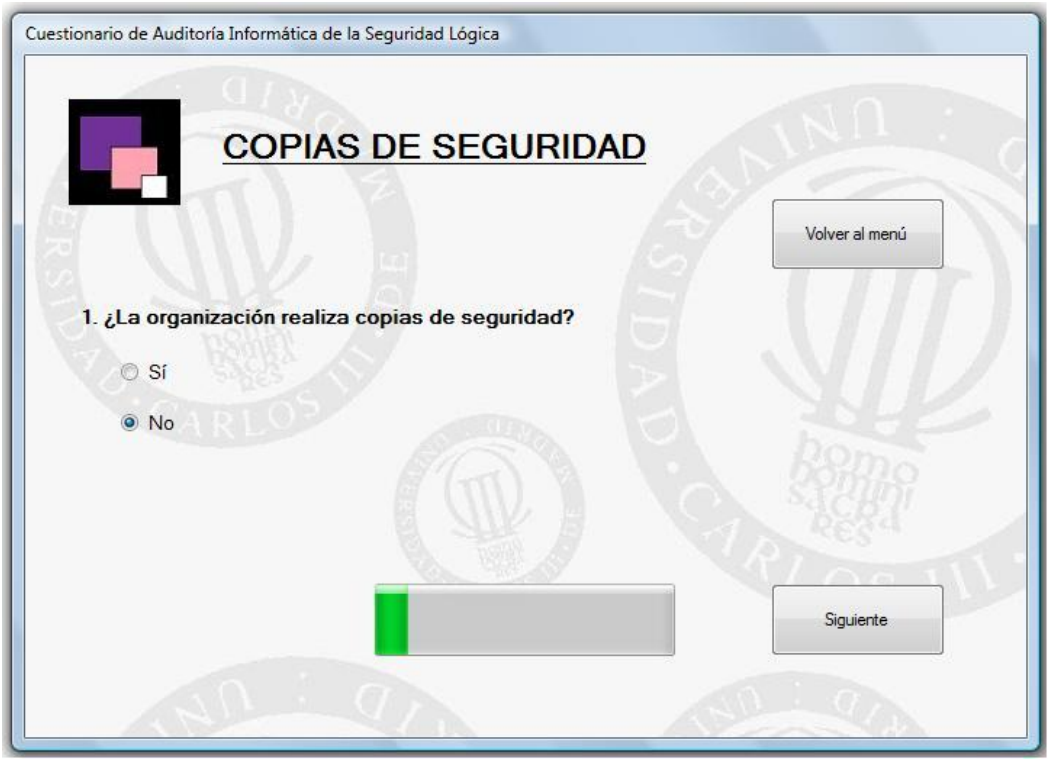
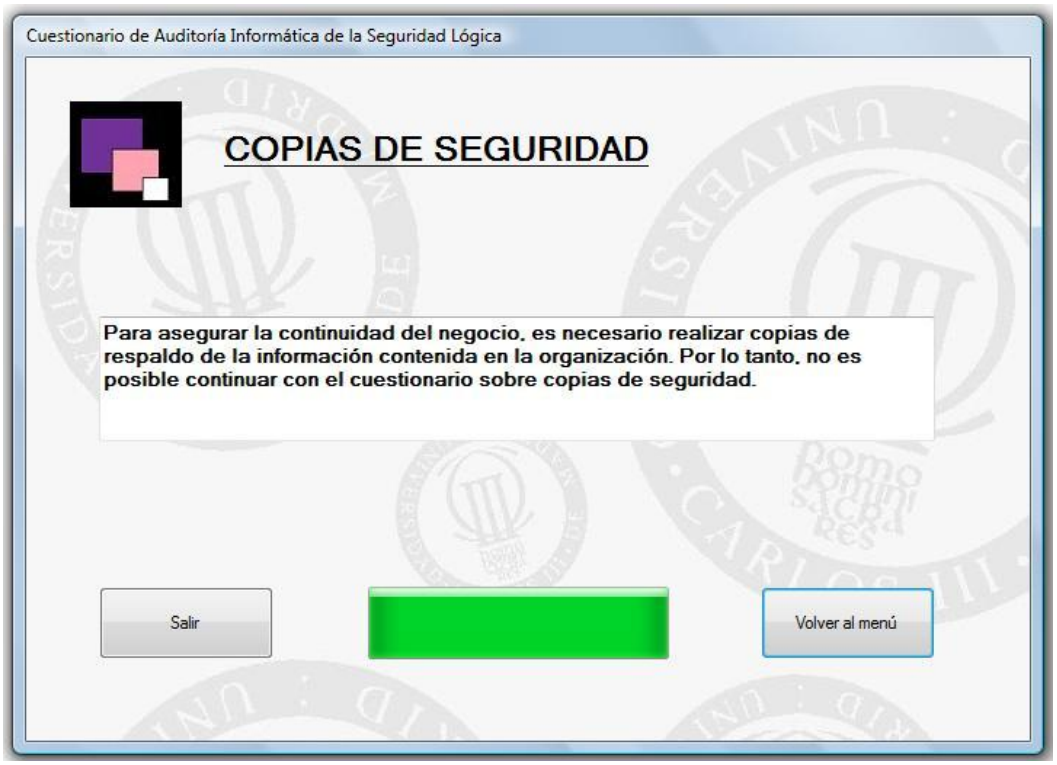


Figura 5.58 Copias de seguridad Advertencia



5. 4. 8 Caso práctico: Copias de seguridad (II)

La compañía "E" realiza copias de seguridad cada tres meses. Los *backups* se realizan siempre en domingo ya que durante ese día, la entidad no muestra actividad. En el caso de que se produjera un fallo en la realización del respaldo, existe un responsable que llevará a cabo las medidas recogidas en el Plan de Contingencia. El resto de empleados no son conscientes de la importancia de la realización de respaldos de la información y la empresa tampoco se ha preocupado en fomentar su comunicación.

De momento, no ha sido necesario utilizar ninguna de las copias de seguridad para restaurar información y la empresa nunca ha probado a restaurar ninguna de estas copias. Los *backups* que contienen información confidencial se tratan de la misma forma que aquellos que contienen el resto de la información de la compañía.

Los procedimientos de realización de copias de respaldo son automatizados pero no se realizan pruebas sobre estos para comprobar que realicen su actividad de forma adecuada.

La empresa está siendo auditada para detectar vulnerabilidades e identificar amenazas y cumplir las recomendaciones que recoja el informe final de su auditoría para aminorar las debilidades. Se dispone a realizar el apartado de "*Copias de seguridad*":

Figura 5.59 Copias de seguridad (II) 1

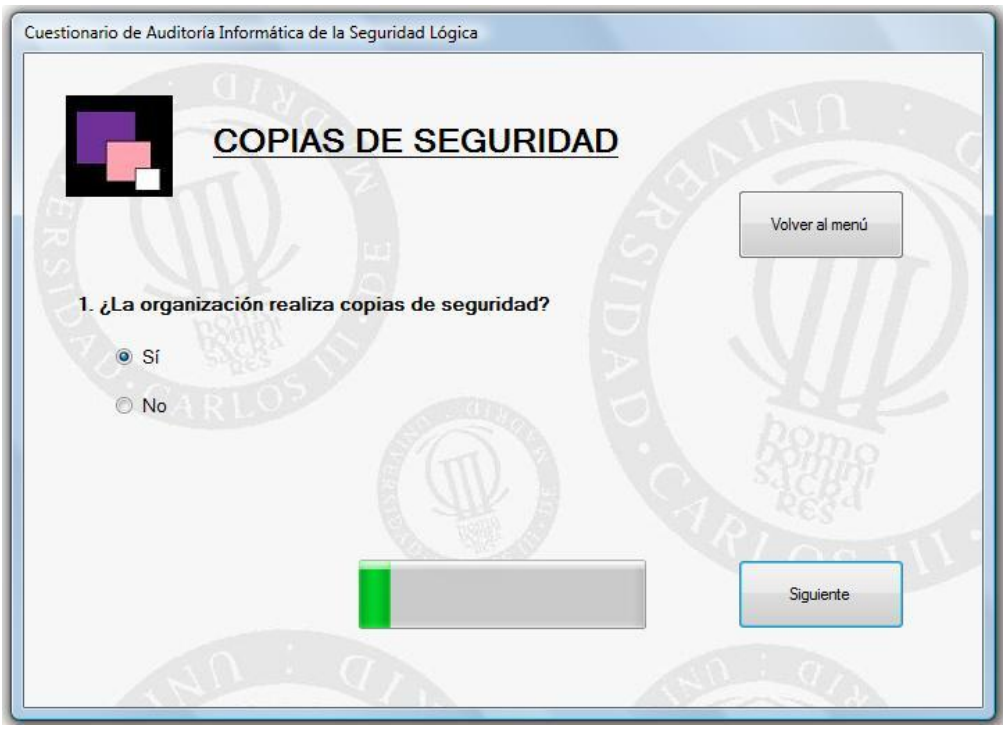


Figura 5.60 Copias de seguridad (II) 2

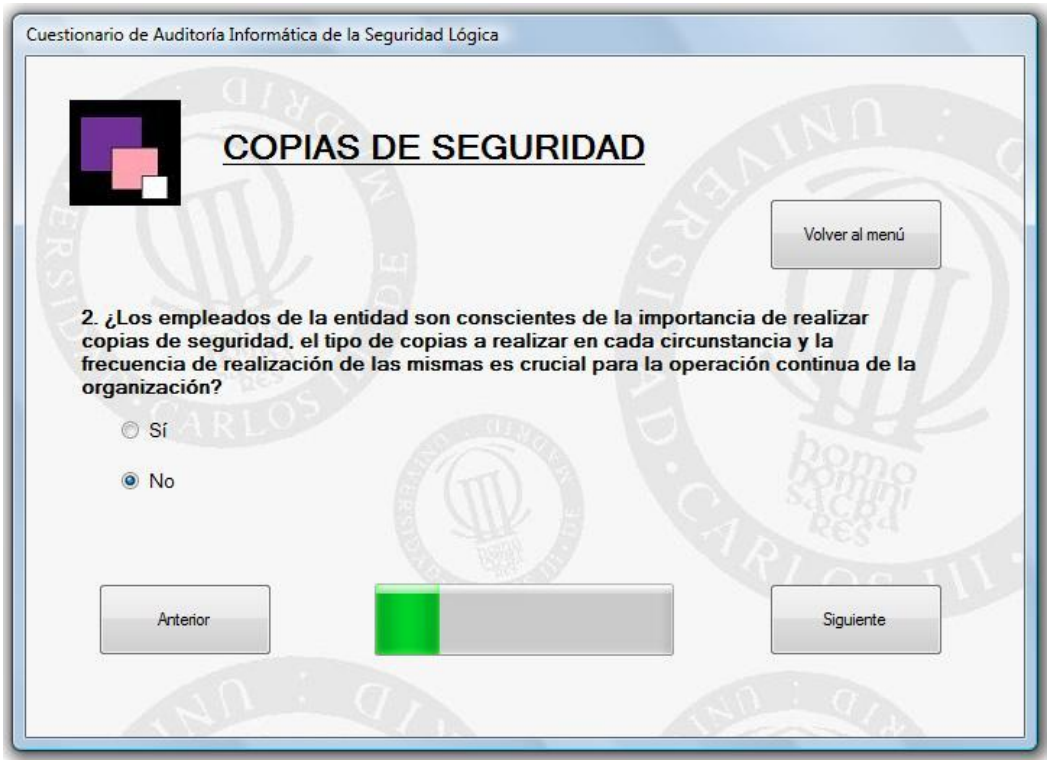


Figura 5.61 Copias de seguridad (II) 3

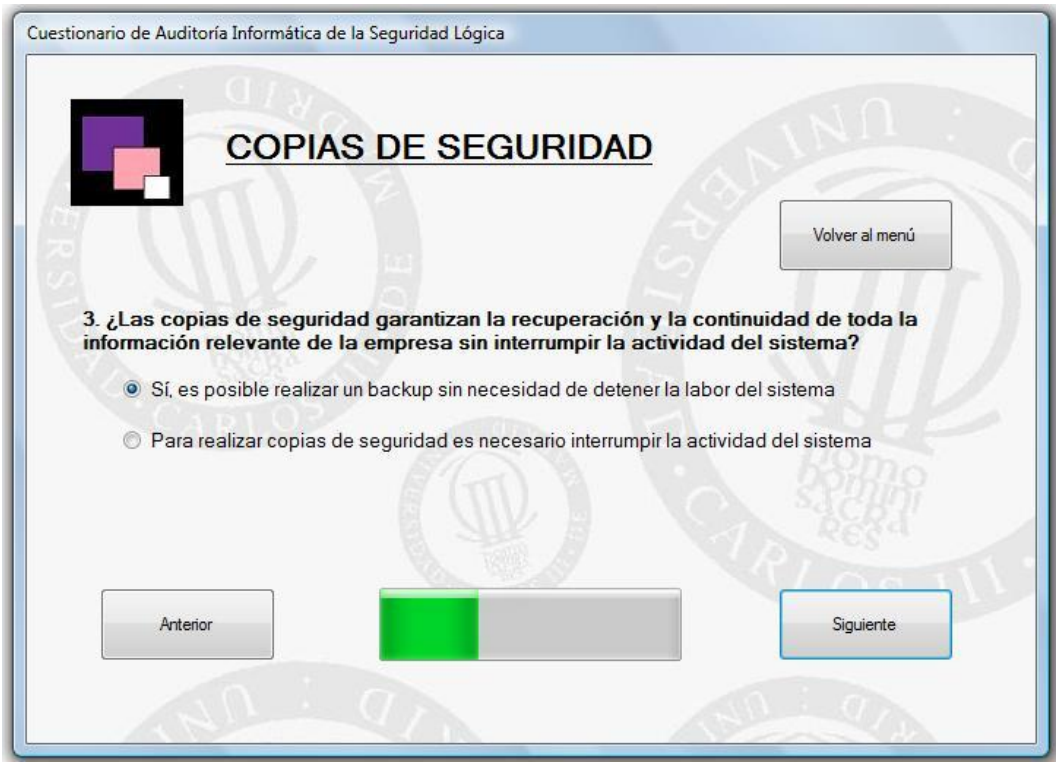


Figura 5.62 Copias de seguridad (II) 4

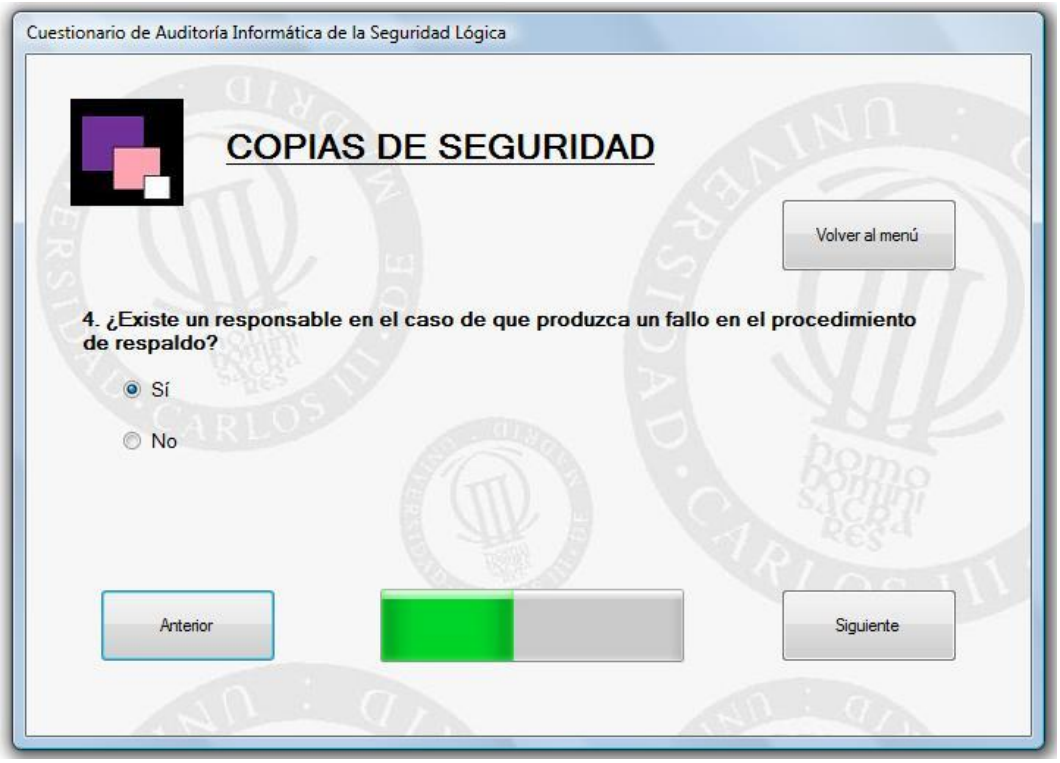


Figura 5.63 Copias de seguridad (II) 5

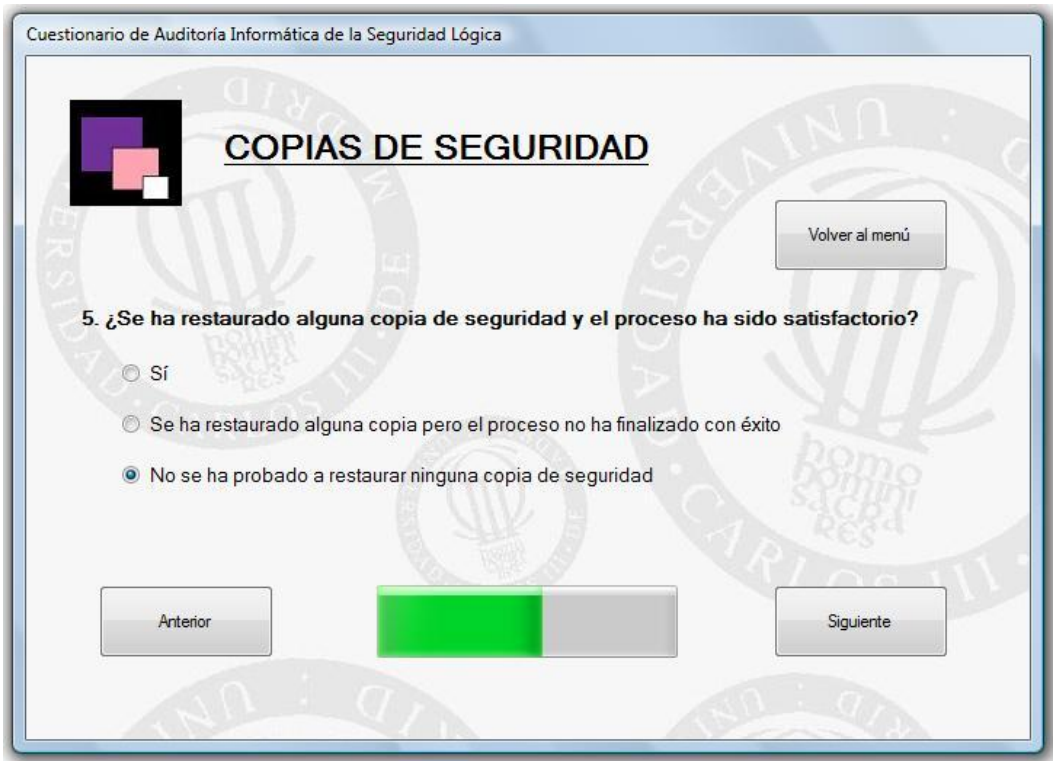


Figura 5.64 Copias de seguridad (II) 6

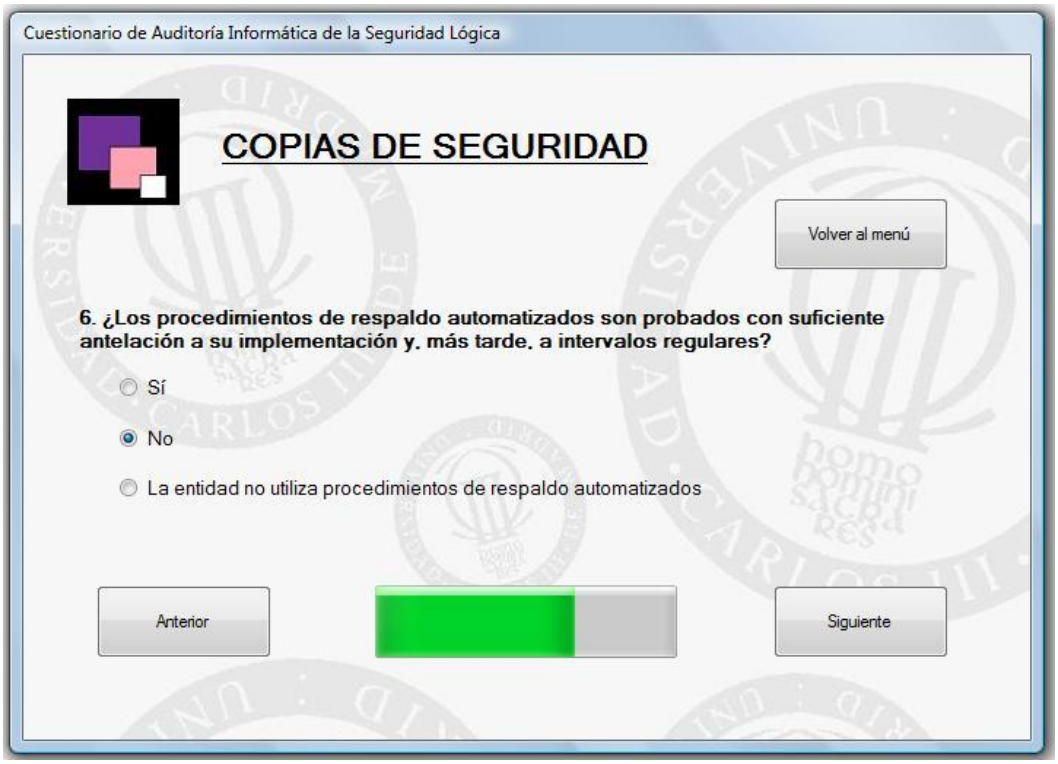


Figura 5.65 Copias de seguridad (II) 7

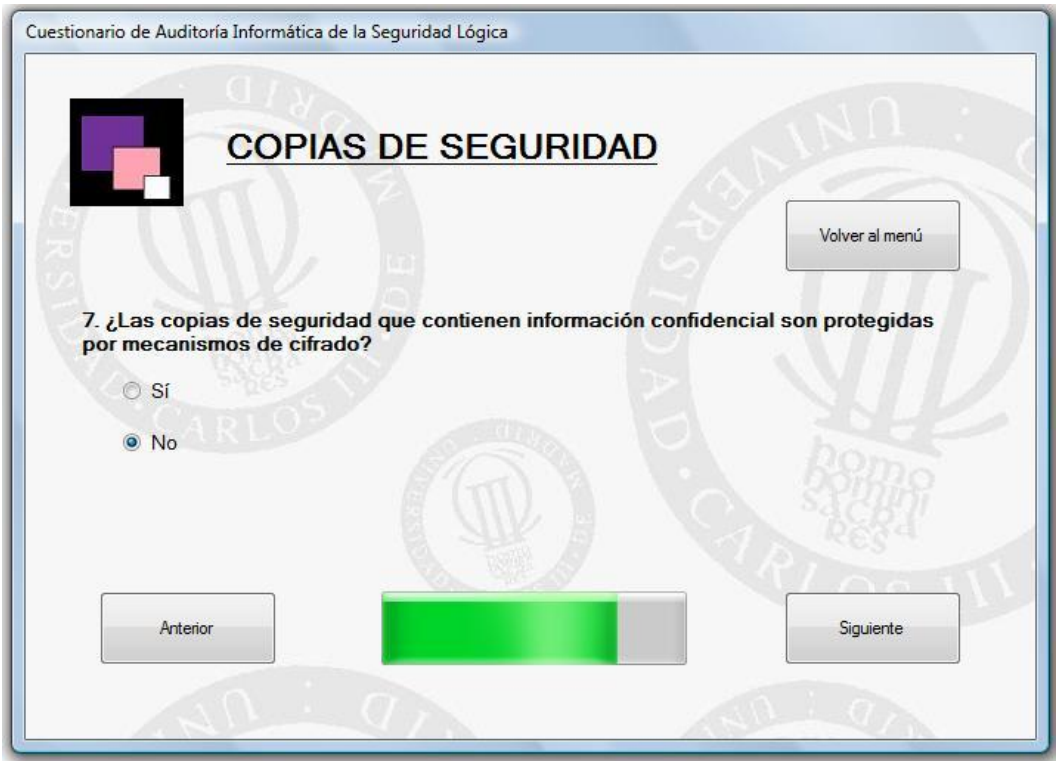


Figura 5.66 Copias de seguridad (II) 8

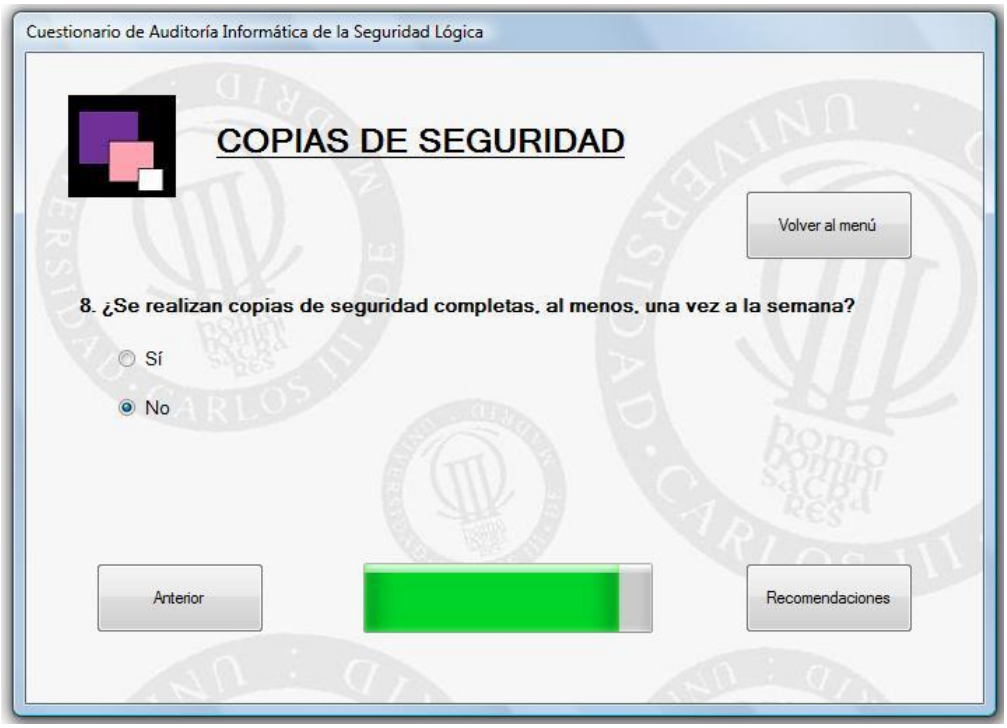
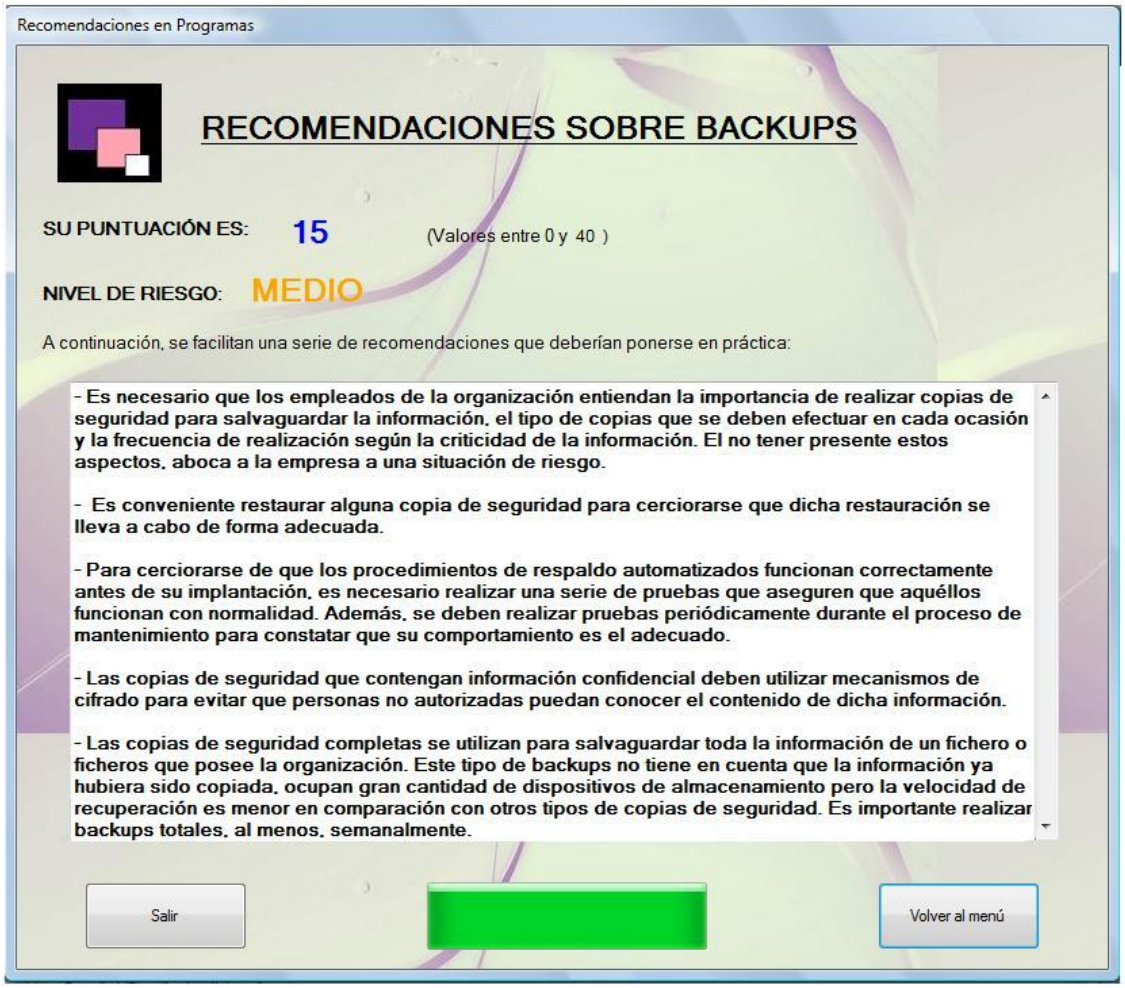


Figura 5.67 Copias de seguridad (II) Recomendaciones



5. 4. 9 Caso práctico: Amenazas lógicas

La empresa "E" hace uso de programas antivirus para detectar virus y otras amenazas lógicas. A día de hoy, ha sufrido algunos ataques con código malicioso que siempre han sido detectados y eliminados sin llegar a repercutir a la organización.

Todos los años, la compañía realiza informes con los ataques sufridos y de los resultados del último año cabe destacar que: la empresa sufrió ataques de modificación de la información, de suplantación de identidad y de intercepción.

Desde hace tres años, la empresa cifra toda la información sensible que circula por la red por si se produce un ataque de intercepción no se pueda conocer dicha información.

La dirección de la compañía está estudiando formar a todos los empleados que utilizan el sistema para reducir considerablemente los ataques sufridos y concienciarlos de la importancia de la seguridad.

Entre las medidas de seguridad implantadas por la empresa, también se encuentra el uso de cortafuegos bien configurados para evitar accesos ilícitos desde Internet y controlar el tráfico de paquetes entre su red privada e Internet.

Los controles de seguridad se revisan y se prueban con frecuencia para asegurarse de que funcionan correctamente. El proceso de contestar a las cuestiones sobre "*Amenazas lógicas*" y las recomendaciones son las siguientes:

Figura 5.68 Amenazas lógicas 1

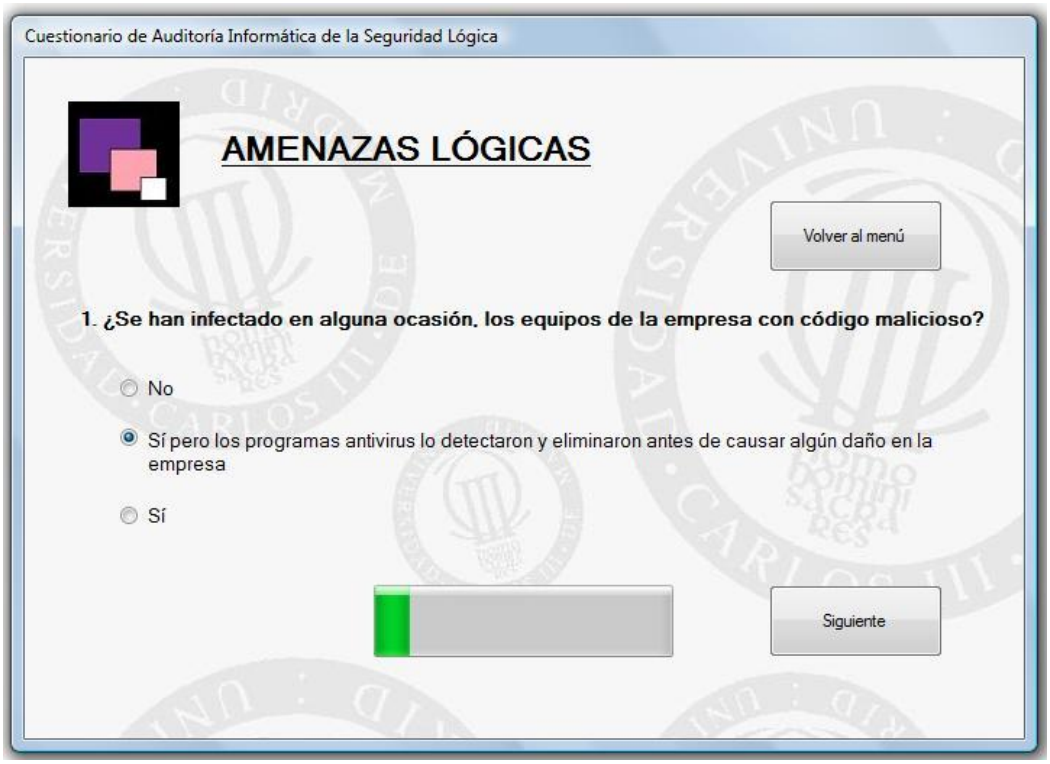


Figura 5.69 Amenazas lógicas 2

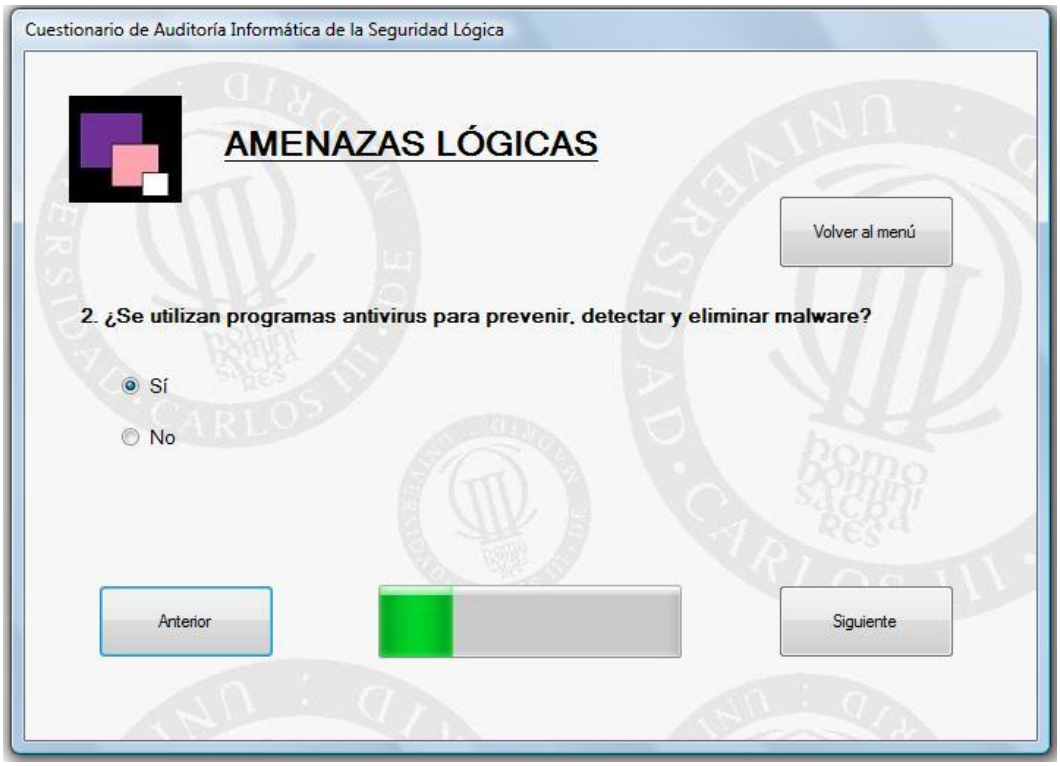


Figura 5.70 Amenazas lógicas 3

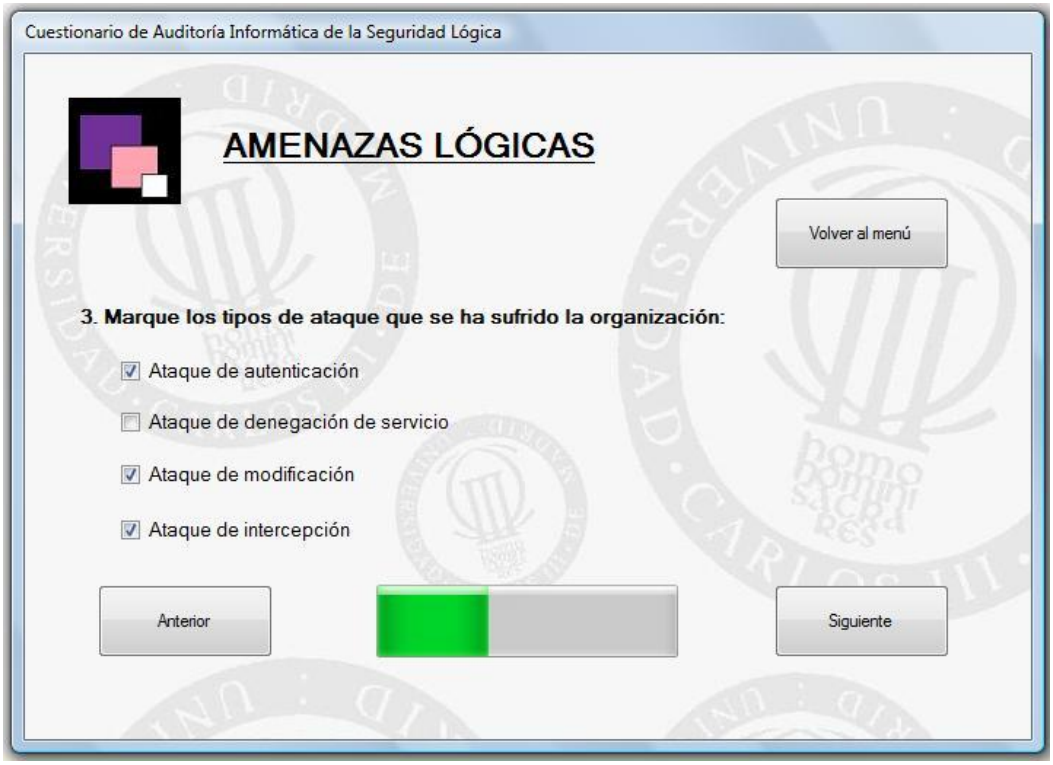


Figura 5.71 Amenazas lógicas 4

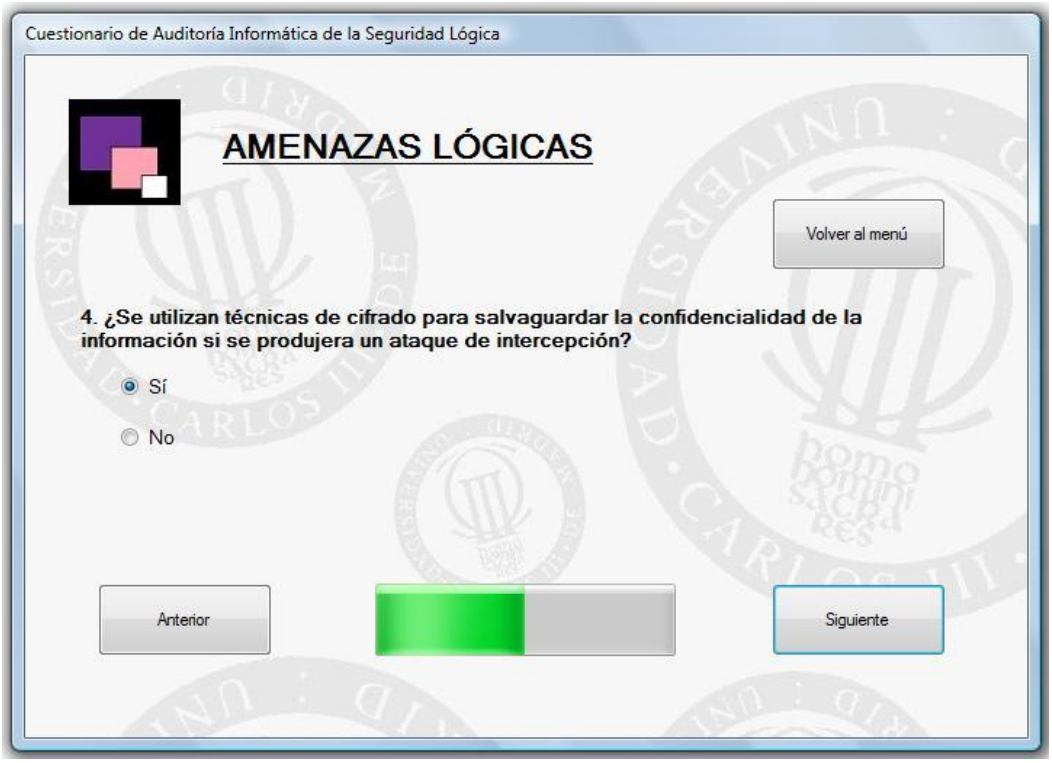


Figura 5.72 Amenazas lógicas 5

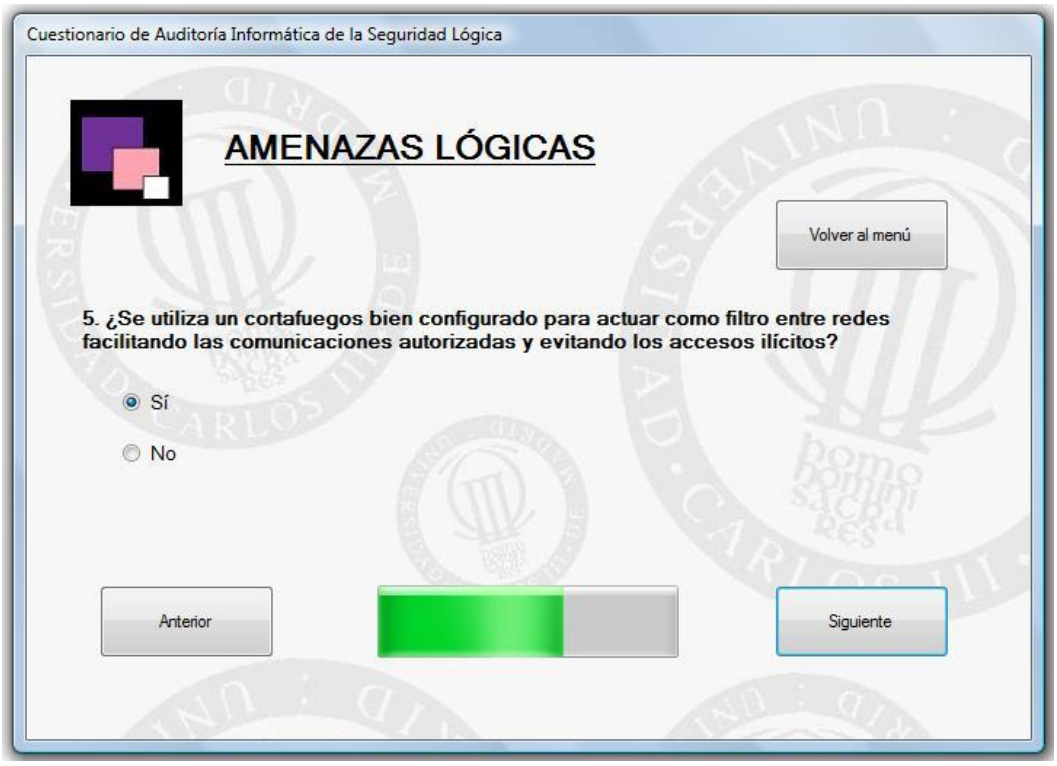


Figura 5.73 Amenazas lógicas 6

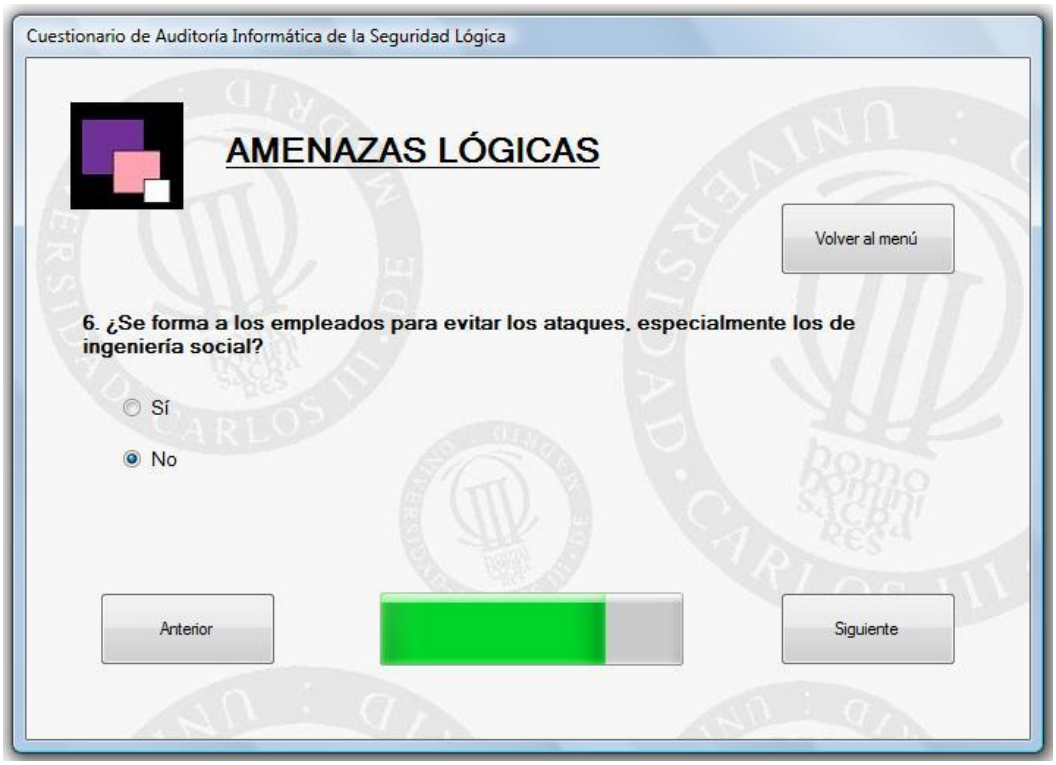


Figura 5.74 Amenazas lógicas 7

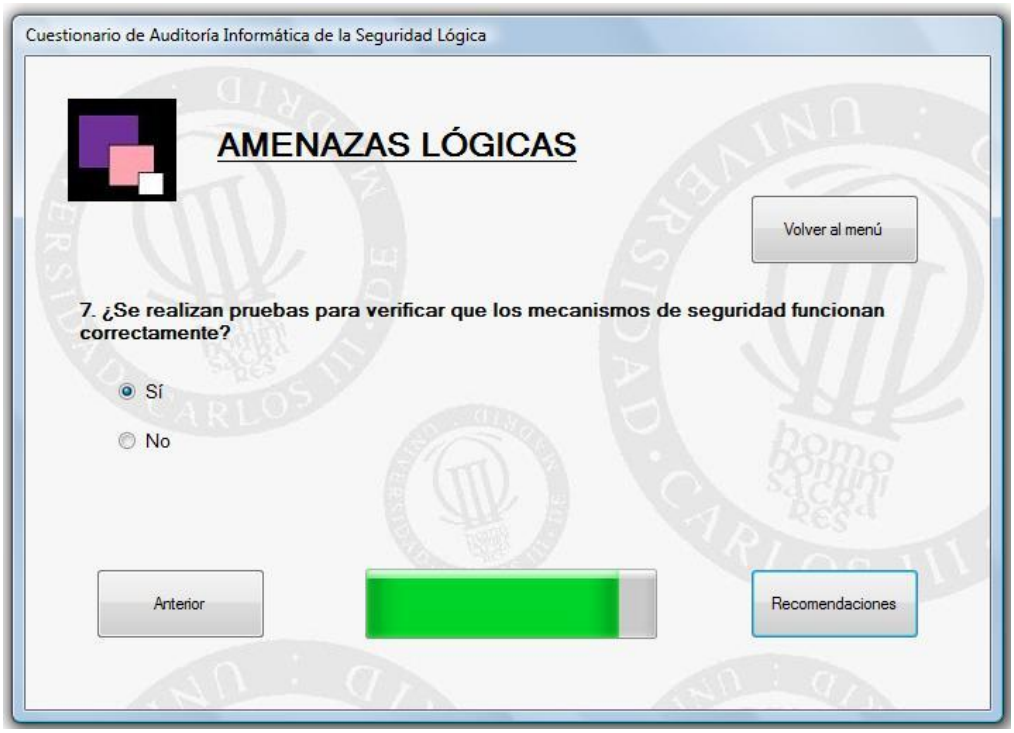
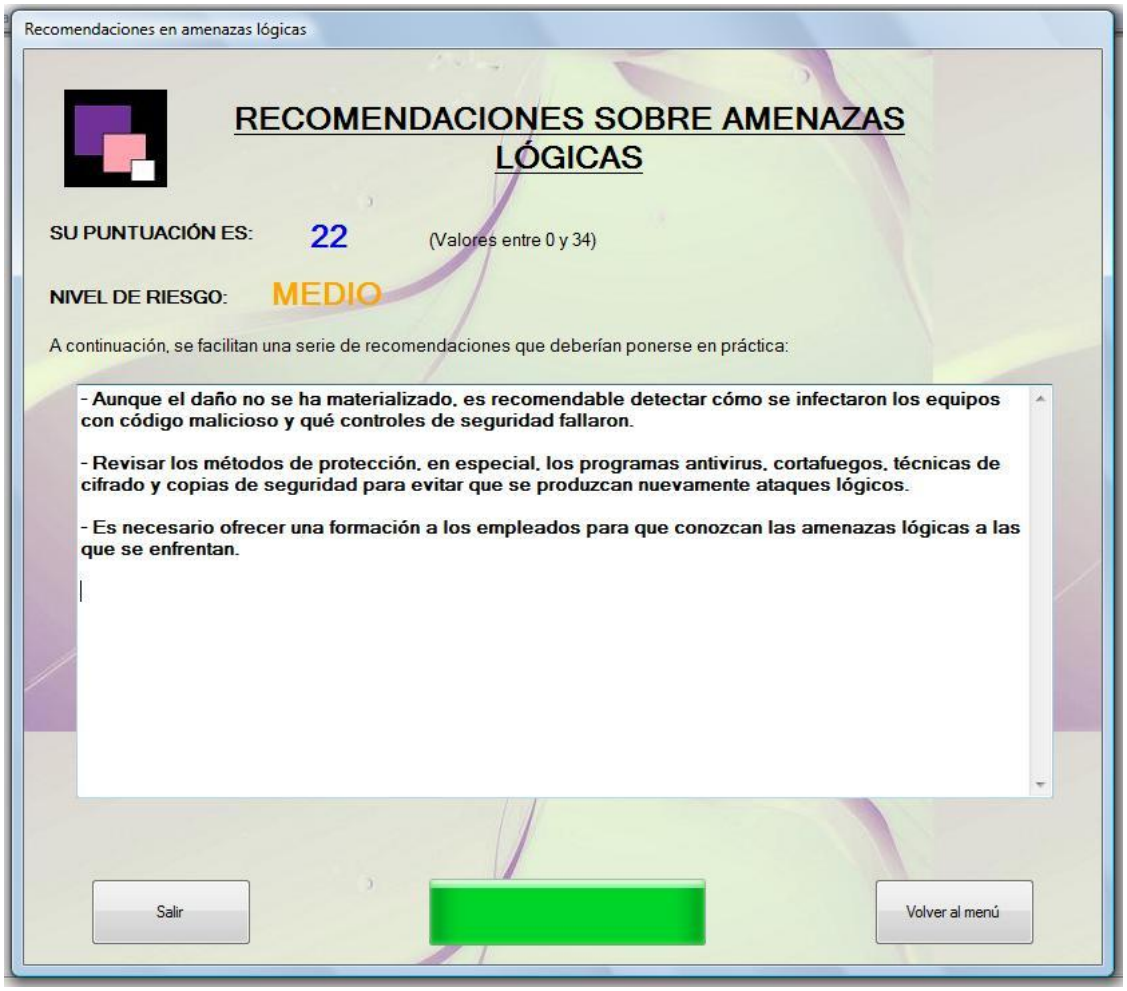


Figura 5.75 Amenazas lógicas Recomendaciones



5. 4. 10 Caso práctico: Programas

La empresa "F" es una pequeña compañía de 20 trabajadores. En las cuentas de los últimos meses, se refleja que existen más pérdidas que ganancias. Algunos empleados necesitar programas para desempeñar su actividad que la empresa no ha adquirido todavía.

Debido a esto, algunos trabajadores decidieron descargar los programas de Internet forma ilegal para evitar el pago de la licencia. Puesto que el *software* no es legal, no son informados de las últimas versiones o parches que existe en el mercado.

El *software* antivirus también es de origen desconocido y la organización tampoco recibe sus actualizaciones. Todos los empleados tienen acceso a cualquier programa instalado en sus computadoras.

Los resultados obtenidos por la empresa del apartado de "*Programas*" es el siguiente:

Figura 5.76 Programas 1

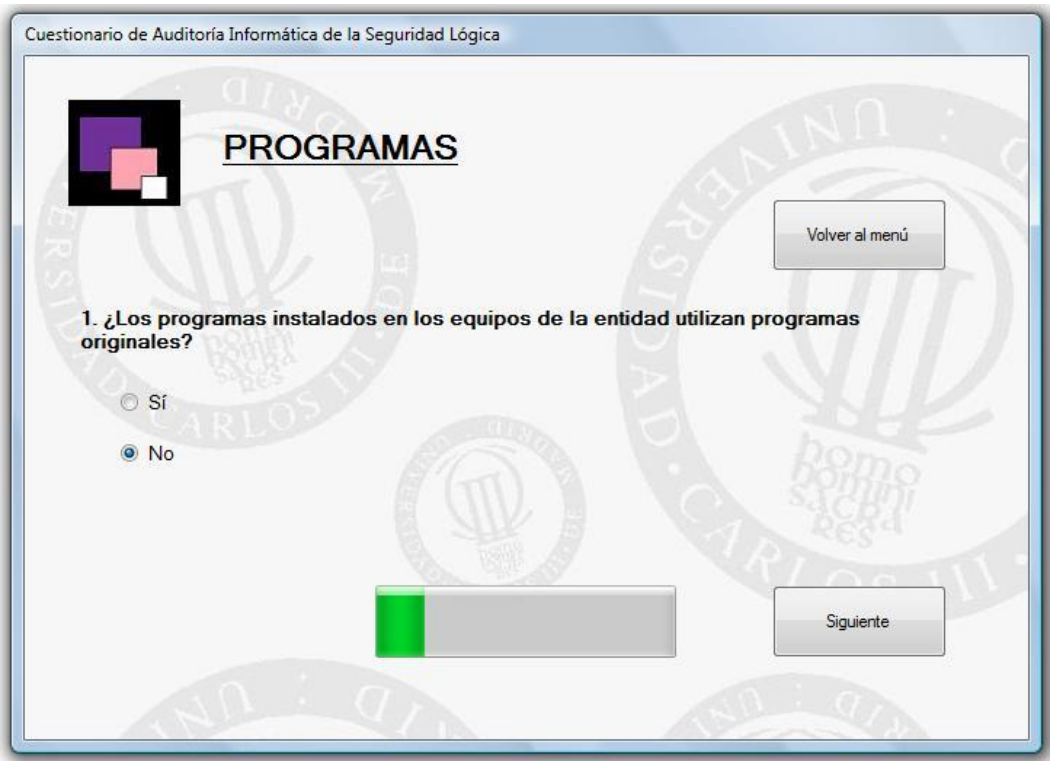


Figura 5.77 Programas 2

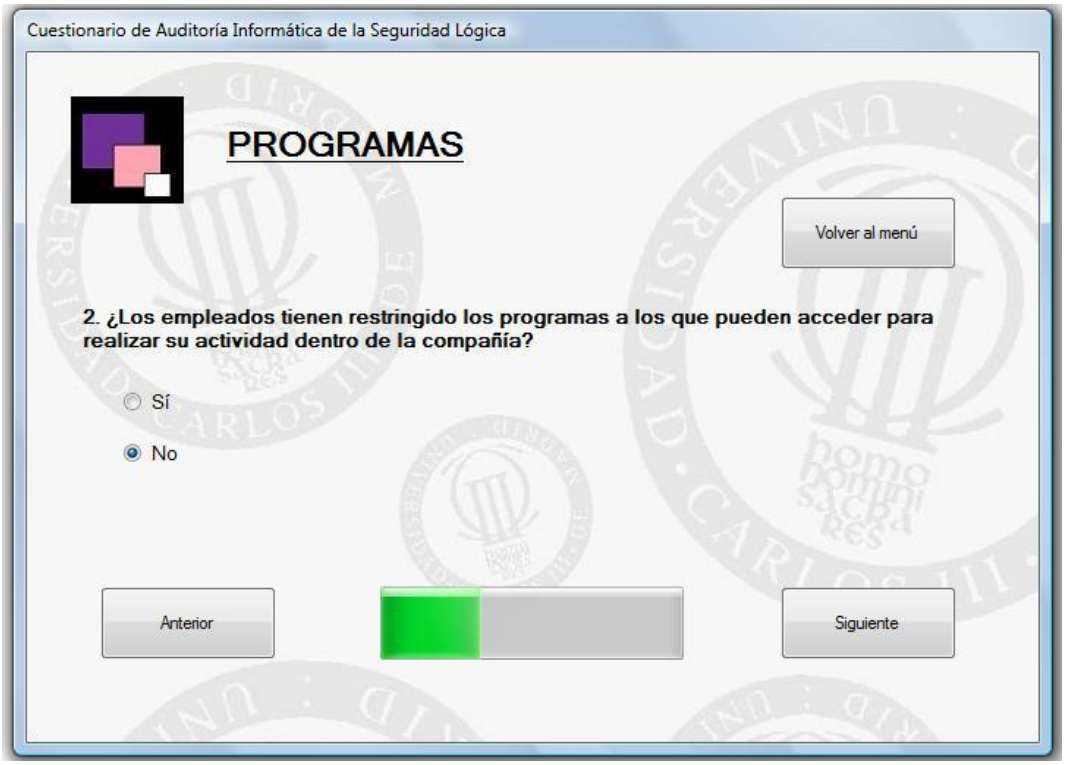


Figura 5.78 Programas 3

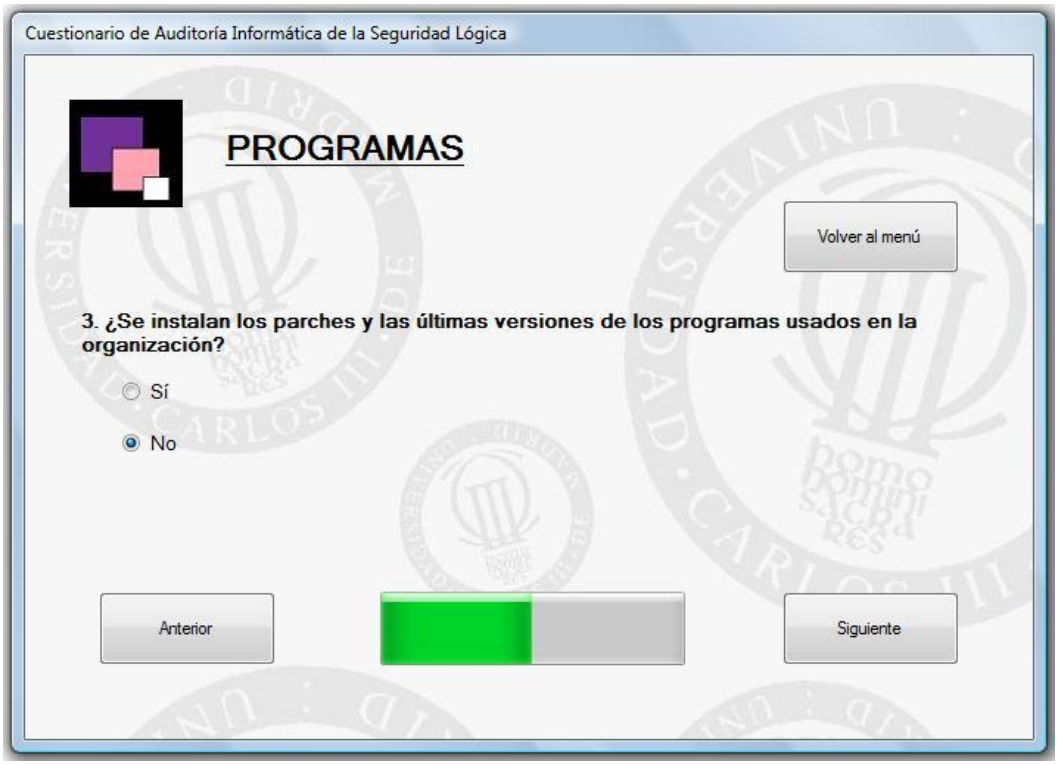


Figura 5.79 Programas 4

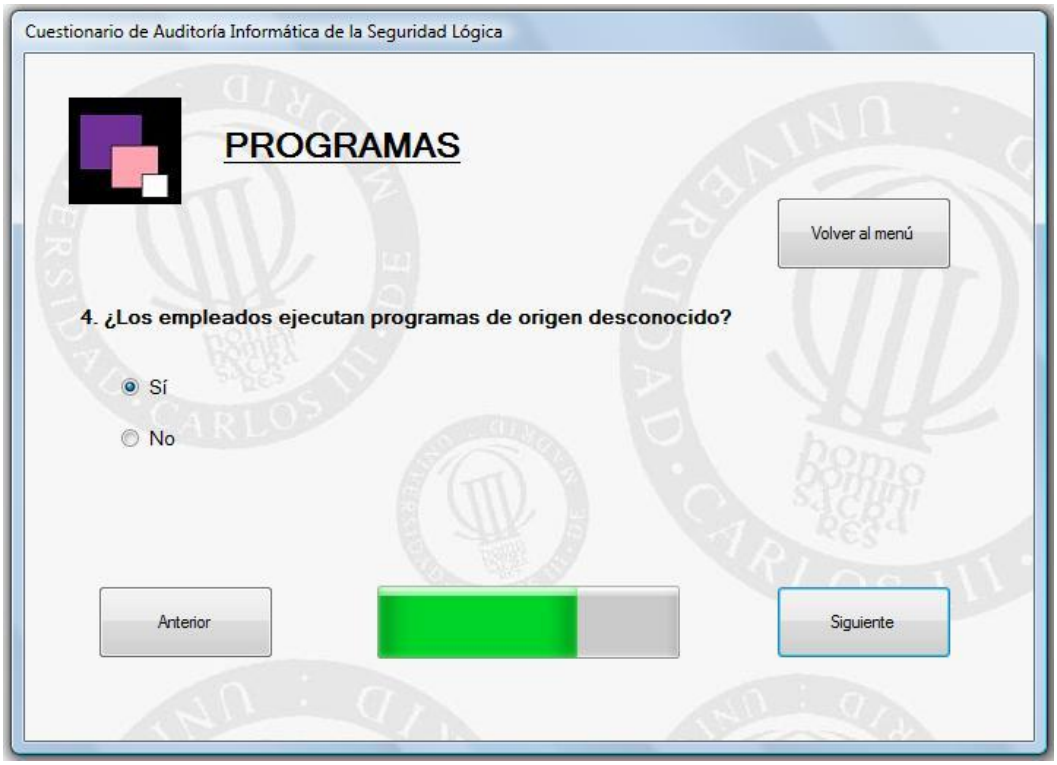


Figura 5.80 Programas 5

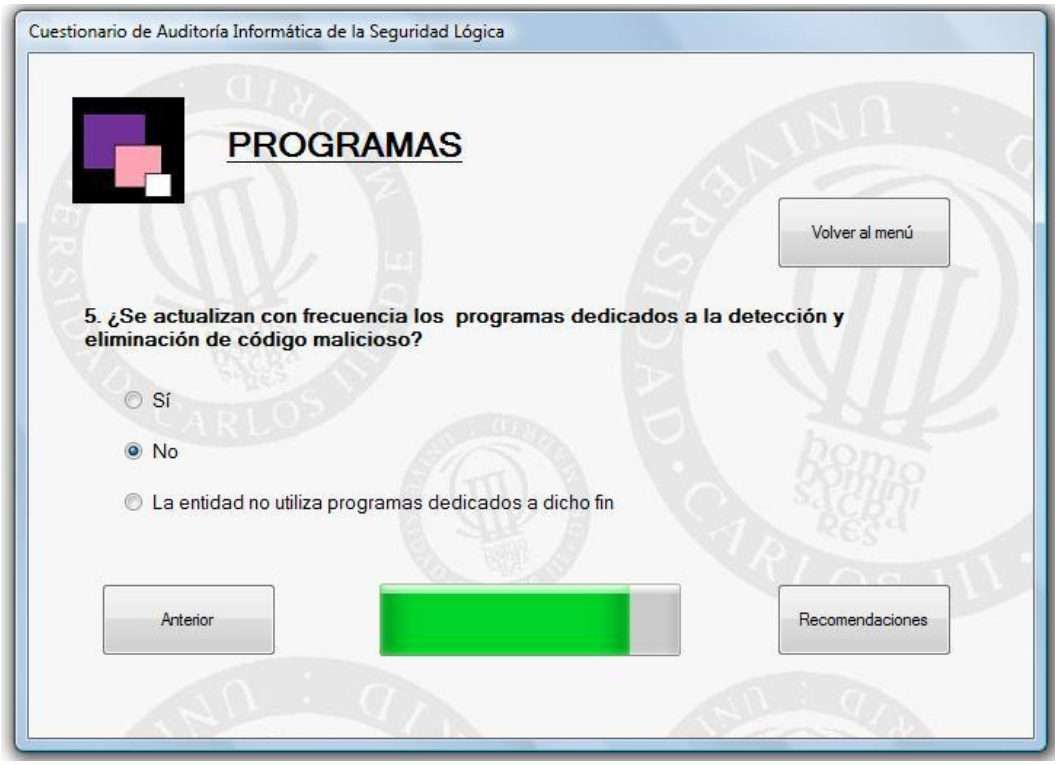
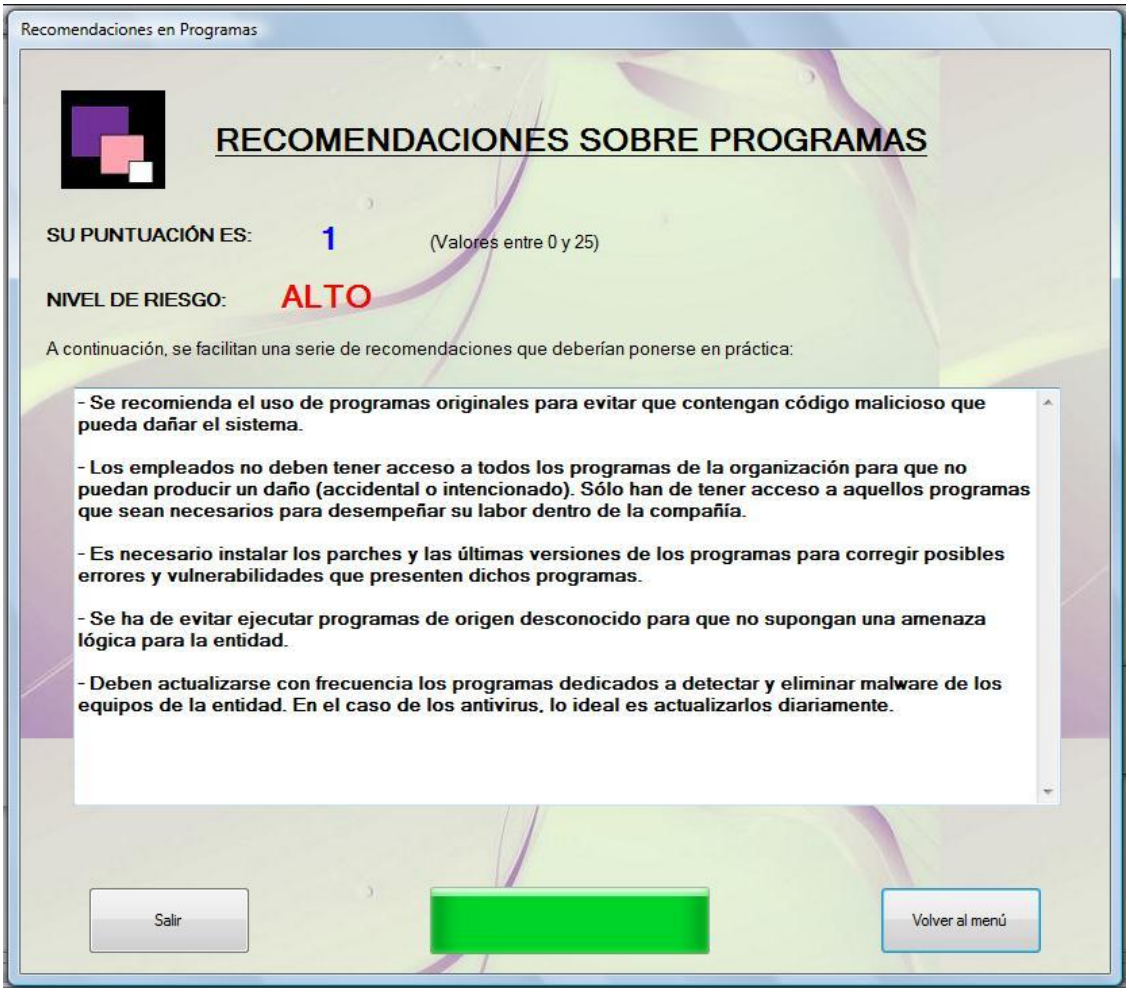


Figura 5.81 Programas Recomendaciones



VI. CONCLUSIONES

Se consideran los **objetivos marcados** al inicio de este proyecto cumplidos. El objetivo principal era concienciar a las personas y en concreto, a las empresas, de la importancia de la seguridad lógica y de someterse a auditorías para verificar que los controles funcionan correctamente y conocer las debilidades a las que se expone la compañía para poder aplicar soluciones. El éxito de una empresa dependerá en gran medida, del nivel de seguridad aplicado y de esta forma, minimizar la posibilidad de materialización de una amenaza sobre aquélla.

Las **futuras líneas de investigación** podrían ser: ampliar los métodos de protección explicando con mayor detalle los cortafuegos, las copias de seguridad, la criptografía y cualquier otro método de seguridad que surja en los próximos años. También se podría escribir sobre seguridad física y complementar así este documento. Asimismo, a medida que vayan evolucionando las nuevas tecnologías, irán surgiendo nuevas amenazas que deberán ser estudiadas. Referente a la aplicación, es posible introducir mejoras, ampliando los temas y preguntas, priorizando las recomendaciones y adaptándolo el cuestionario a las empresas que se auditen.

A título personal, este Proyecto Fin de Carrera ha supuesto un gran esfuerzo de constancia y muchos momentos duros que ahora se ven recompensados con la finalización de este proyecto. Me ha sido de gran utilidad realizar este trabajo para asentar los conocimientos adquiridos durante estos años en la carrera, es especial, en las materias de auditoría, seguridad y programación. Además, he aprendido a programar en *Microsoft Visual Basic 2008*, lenguaje que he utilizado para implementar el cuestionario de auditoría.

Este proyecto, me ha exigido un largo proceso de documentación y, en ocasiones, la contradicción de fuentes me ha supuesto algún que otro quebradero de cabeza… La frase de "*todo esfuerzo tiene su recompensa*" hoy cobra para mí, más sentido que nunca.

He aportado mi visión sobre la importancia de la seguridad centrándome en la seguridad lógica y de accesos. Además, he creado una aplicación que puede servir de ayuda a un auditor para recabar información en la realización de una auditoría y las recomendaciones que debe plasmar en el informe final.

Respecto al **tiempo dedicado** para realizar este trabajo no puedo estimar con precisión las horas invertidas puesto que ha habido meses en los que he dedicado gran cantidad de horas y otros que por diversos motivos, no han sido tantas como hubiese querido.

Invertí gran cantidad de horas en el comienzo de esta memoria para hacerme una idea de qué iba plasmar en este documento y en leer abundante documentación para que la información fuera lo más rigurosa posible.

Para concluir, solamente destacar que hago una valoración positiva de los conocimientos aprendidos y puestos en práctica a través de este duradero y arduo trabajo, que ha hecho que su propia finalización supusiera para mí, un verdadero reto personal.

GLOSARIO DE TÉRMINOS

Activo: recurso que posee una empresa para el desarrollo de su actividad y como resultado de las operaciones diarias que en un futuro se materializan en beneficios económicos.

AEPD: Agencia Española de Protección de Datos.

Adware: aplicación que muestra publicidad.

Amenaza: evento que puede desencadenar un daño.

Amenaza lógica: programas que pueden dañar el sistema, creados intencionadamente o por error.

Análisis: diferenciar y desmembrar las partes de un todo hasta averiguar sus principios o elementos.

Análisis de sistemas: determinar los objetivos, límites, estructura y funcionamiento del sistema estudiado, y la interacción con otros sistemas.

Análisis de escenario: explora contextos futuros alternativos. Puede probar la estabilidad de la estrategia de la empresa, analizar posibles desarrollos en el mercado o incrementar las oportunidades de éxito abordando futuros inciertos, entre otras cosas.

Applet: aplicación escrita generalmente en Java que se ejecuta en un navegador web.

Atacante: persona que perjudica o causa un daño.

Ataque asincrónico: aprovecha cualquier posibilidad que ofrezca el sistema operativo de reiniciar el sistema para desviar datos relevantes.

Auditor: persona independiente encargada de llevar a cabo una auditoría.

Auditoría informática: "*proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo los fines de la organización y utiliza eficientemente los recursos*". [Ron Weber]

Autenticar: asegurar que un documento u hecho es verdadero.

Backdoor: véase *Puerta trasera*.

Backup: véase *Copia de seguridad*.

Biometría: tecnología de identificación de personas basada en el reconocimiento de unas características físicas o conductuales.

Bomba lógica: programa que se activa después de un cierto periodo de tiempo causando algún daño al sistema.

Brainstorming: véase *Tormenta de ideas*.

Bug: error o defecto en un programa.

Caballo de Troya: instrucciones escondidas en un programa que realiza acciones maliciosas sin que el usuario tenga conocimiento de esto.

Canal oculto o encubierto: canal de comunicación que infringe la política de seguridad del sistema, y permite a dos procesos intercambiar información de forma ilegítima.

Carding: uso ilícito de tarjetas de crédito ajenas.

Catástrofe: suceso nefasto que altera el orden normal de las cosas.

COBIT: conjunto de buenas prácticas para el control de la información, las tecnologías de la información y los riesgos que conllevan.

Comunicación: acción y resultado de comunicar o comunicarse.

Confidencialidad: cualidad de un documento o mensaje que sólo puede ser leído por personas autorizadas.

Consecuencia: hecho o suceso que se deriva o resulta de otro.

Contraseña: clave para permitir o restringir el acceso a un determinado lugar, sistema o fichero.

Control: actividad o acción para prevenir, detectar o corregir errores y anomalías que puedan afectar al funcionamiento correcto del sistema.

Cookie: fragmento de información personal del usuario almacenada en el disco duro para conseguir una navegación más personalizada.

Copia de seguridad: se utiliza para recuperar la información del sistema en el caso de pérdida o fallo.

Cortafuegos: filtro entre redes con el fin de facilitar las comunicaciones autorizadas y evitar los accesos ilícitos.

Covert channel: véase *Canal oculto*.

Criptografía: escribir con clave secreta o de forma enigmática.

Daño: perjuicio o deterioro personal o material.

Data diddling: consiste en alterar datos sin autorización.

Data leakage: sustraer información relevante con fines deshonestos.

Dato: información que permite una deducción o conocimiento exacto.

Denegación de servicio (DoS): imposibilidad que tiene un usuario autorizado de acceder a un recurso o servicio.

Denial of Service: véase *Denegación de servicio*.

Diagramas de flujo: representación gráfica que permite entender con mayor claridad los pasos de un proceso.

Exploit: técnica que se encarga de aprovechar los errores que contiene un programa.

Firewall: véase *Cortafuegos*.

Firma electrónica: es un conjunto de datos en forma electrónica, que se añaden a otros datos para identificar formalmente al firmante del documento.

Función crítica: aquella función cuya interrupción, pasado un determinado periodo de tiempo, supone un impacto para la compañía.

Fungible: elemento que se gasta o se desgasta con el uso.

Gusano: programa que se ejecuta y se propagar por sí mismo a través de una red.

***Hardware* (Hw)**: componentes físicos del ordenador y sus periféricos.

Identificación: reconocimiento de la identidad de un individuo.

Impacto: consecuencia del daño derivado de la materialización de una amenaza en la organización.

Incertidumbre: inseguridad o grado de desconocimiento.

Incidente: suceso o circunstancia que interfiere en el transcurso normal de algo.

Información: conjunto de datos que permiten adquirir algún tipo de conocimiento.

Ingeniería social: técnica que consiste en manipular a las personas para que realicen actos de forma voluntaria que de otro modo no harían.

Interrupción: pausa en el progreso o continuidad de algo.

Juicio de experiencia: valoración formada por un conjunto de percepciones.

Kerberos: protocolo de autenticación que permite identificar ordenadores de forma fiable en una red no segura.

LOPD: Ley 15/1999 de Protección de Datos de carácter personal.

LSSICE: Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico.

Mecanismos de Seguridad: controles diseñados para prevenir, detectar o recuperarse de un ataque de seguridad.

Organigrama: representación gráfica que permite obtener una idea de la estructura organizativa de una empresa.

Password: véase *Contraseña*.

Pharming: consiste en manipular las direcciones DNS a las que accede el usuario, y redirigir un nombre de dominio a otra máquina.

Phishing: suplantación de identidad a través de correos electrónicos o páginas web para conseguir datos personales.

Plan de Contingencias: guía detallada de cómo se debe actuar ante determinados eventos que se produzcan en la organización, a fin de asegurar la continuidad del negocio.

Política de seguridad: reglas y procedimientos que constituyen la base del entorno de seguridad de una organización.

Programa bacteria: programa que se reproduce hasta agotar los recursos del ordenador causando una denegación del servicio.

Programa conejo: véase *Programa bacteria*.

Puerta trasera: permite el acceso a una máquina de manera remota sin el consentimiento del usuario.

P2P: o red *peer-to-peer* es una red de ordenadores en la que éstos se comportan como iguales entre si, es decir, actúan simultáneamente como clientes y servidores. Generalmente estas redes se utilizan para compartir ficheros de cualquier tipo.

Recogida de información residual: sustraer información depositada en las papeleras.

Red: conjunto de ordenadores conectados entre sí.

Riesgo: daño o peligro al que está expuesto una entidad.

Rootkit: conjunto de herramientas para acceder a un sistema sin autorización del usuario.

Scavenging: véase *Recogida de información residual*.

Scam: mensaje enviado a través del correo electrónico que contiene una propuesta con el fin de estafar económicamente al usuario.

Seguridad: sentimiento de protección frente a daños y peligros.

Seguridad física: aplicación de barreras físicas y procedimientos para proteger a la compañía de ataques físicos en los equipos, documentación, instalaciones, personal, etc.

Seguridad lógica: aplicación de barreras y procedimientos que protejan el acceso a los datos procesos y programas, y sólo tengan acceso a ellos personas autorizadas.

Sistema de Información (SI): conjunto de elementos que interactúan entre si para procesar y distribuir los datos y la información con el fin de cumplir unos objetivos.

Sniffing: captura de paquetes que circulan por la red.

***Software* (Sw)**: conjunto de programas, aplicaciones y sistemas operativos que permiten que el hardware funcione.

***Software* espía**: véase *Spyware*.

Spam: mensaje publicitario enviado por correo electrónico a gran cantidad de usuarios sin solicitarlo.

Spoofing: suplantación de una identidad para llevar a cabo acciones ilícitas sobre un sistema.

Spyware: *software* que envía información personal del usuario sin su consentimiento a terceros.

Superzapping: "llave maestra" que elude los controles y permite el acceso a los ficheros del ordenador.

Tampering: véase *Data diddling*.

Técnica del salami: consiste en desviar pequeñas cantidades de dinero de diversas fuentes de forma que los afectados nos perciban el robo de una pequeña cantidad.

Time bomb: véase *Bomba lógica*.

Tormenta de ideas: técnica de grupo utilizada para generar nuevas ideas sobre un tema o problema determinado en un ambiente relajado.

Trashing: véase *Recogida de información residual*.

Troyano: véase *Caballo de Troya*.

Virus: secuencia de código que se aloja en un fichero ejecutable que cuando se ejecuta realiza la acción para la que fue programado.

Vulnerabilidad: posibilidad de materialización de una amenaza.

Worm: véase *Gusano*.

BIBLIOGRAFÍA

- Calle Guglieri, J.A. "*Reingeniería y seguridad en el ciberespacio*" (1997). Editorial Díaz de Santos, S.A.

- COBIT 4.1 (2007).

- Corrales Hermoso, Alberto Luis. Beltrán Pardo, Marta. Guzmán Sacristán, Antonio. "*Diseño e implantación de arquitecturas informáticas seguras: una aproximación práctica*" (2006). Ediciones Dykinson.

- Creus Solé, Antonio. "*Fiabilidad y seguridad: su aplicación en procesos industriales*" (2005). Editorial Marcombo, S.A.

- Delgado Rojas, Xiomar. "*Auditoría Informática*" (1998). Editorial Universidad Estatal a Distancia.

- Estándar Internacional ISO/IEC 17799 versión 2005 (actualmente denominada ISO/IEC 27002).

- España Boquera, María Carmen. "*Servicios avanzados de telecomunicación*" (2003). Editorial Díaz de Santos, S.A.

- Gaspar Martínez, Juan. "*Planes de Contingencia: La continuidad del negocio en las organizaciones*" (2004). Editorial Ediciones Díaz de Santos, S.A.

- Gestión informática de los Recursos Humanos. Universidad Carlos III de Madrid.

- "*Informática para las Oposiciones a la Comunidad Autónoma de las Illes Balears*" (2002). Editorial MAD-Eduforma.

- La Fundación Eca Global. "*El auditor de calidad*" (2006). Editorial Fundación Confemetal.

- Lawrence Pfleeger, Shari. P. Pfleeger, Charles. "*Security in computing*" (2006). Editorial Prentice Hall.

- MAGERIT versión 2, libro I "*Método*" (2006). Ministerio de Administraciones Públicas.

- Minguet, Jesús. Read, Tim. "*Informática Fundamental*" (2008). Editorial Centro De Estudios Ramón Areces, S.A.

- Morera Pascual, Juan. Pérez-Campanero Atanasio, Juan. "*Conceptos de sistemas operativos*" (2002).Universidad Pontificia Comillas.

- Pablos Heredero, Carmen de. López-Hermoso, José Joaquín. Martín-Romo, Santiago. Medina, Sonia. "*Informática y comunicaciones en la empresa*" (2004). Editorial ESIC.

- Patrick, Antouly "*Navegue sin riesgos: proteja su ordenador. Virus, spyware, troyanos, piratas, spam*" (2005). Editorial Ediciones ENI.

- Peso Navarro, Emilio del. "*Manual de outsourcing informático: (análisis y contratación)*" (2003). Editorial Ediciones Díaz de Santos, S.A.

- Peso Navarro, Emilio del. Fernández Sánchez, Carlos Manuel. "*Peritajes informáticos*" (2001). Editorial Ediciones Díaz de Santos, S.A.

- Peso Navarro, Emilio del. Ramos González, Miguel Ángel. Peso Ruiz, Mar del. "*El documento de seguridad: (análisis técnico y jurídico. Modelo)*" (2004). Editorial Ediciones Díaz de Santos, S.A.

- Ramos Álvarez, Benjamín. Apuntes de la asignatura "*Seguridad y protección de la información*" de la titulación Ingeniería Técnica en Informática de Gestión (2007). Universidad Carlos III de Madrid.

- Ramos González, Miguel Ángel. Apuntes de la asignatura "*Auditoría informática*" de la titulación Ingeniería Técnica en Informática de Gestión (2007). Universidad Carlos III de Madrid.

- Royer, Jean-Marc. "*Seguridad en la informática de empresa: riesgos, amenazas, prevención y soluciones*" (2004). Editorial Ediciones ENI.

- Stallings, William. "*Fundamentos de seguridad en redes: aplicaciones y estándares*" (2004). Editorial Prentice Hall.

- Vilar Barrio, José Francisco. "*La auditoría de los sistemas de gestión de la calidad*" (2001). Editorial Fundación Confemetal.

- VV.AA. "*Diccionario de Internet*" (2002). Editorial Complutense.

Páginas web consultadas:

http://es.tldp.org/

http://www.isaca.org/

http://www.ibiblio.org/

http://es.wikipedia.org/

http://www.alfa-redi.org/

http://www.coladic-rd.org/

http://www.pandeblog.org/

http://www.kriptopolis.org/

http://www.internautas.org/

http://www.desenredando.org/

http://www.seguridadenlared.org/

http://bitelia.com/

http://elgeek.com/

http://diariored.com/

http://www.ibm.com/

http://www.cicei.com/

http://www.alipso.com/

http://www.popsci.com/

http://www.acceso.com/

http://www.baquia.com/

http://www.laneros.com/

http://www.instisec.com/

http://es.trendmicro.com/

http://www.pcworld.com/

http://www.hispasec.com/

http://uw713doc.sco.com/

http://www.geocities.com/

http://www.virusprot.com/

http://www.sallandre.com/

http://www.fasecolda.com/

http://www.microsoft.com/

http://www.mailxmail.com/

http://rsolis.wordpress.com/

http://www.gestiopolis.com/

http://www.noticiasdot.com/

http://www.vsantivirus.com/

http://www.tuguialegal.com/

http://auditoriasistemas.com/

http://www.perantivirus.com/

http://lordhash.blogspot.com/

https://www.cenitsegura.com/

http://www.masadelante.com/

http://www.infospyware.com/

http://www.planetcursos.com/

http://www.zonagratuita.com/

http://www.monografias.com/

http://www.wikilearning.com/

http://www.microsiervos.com/

http://www.empresuchas.com/

http://www.todoexpertos.com/

http://www.adrformacion.com/

http://www.pandasecurity.com/

http://antivirus.interbusca.com/

http://www.programatium.com/

http://diccionario.babylon.com/

http://www.basc-costarica.com/

http://www.mitecnologico.com/

http://www.wordreference.com/

http://www.ciencia-ficcion.com/

http://www.formacion3000.com/

http://www.bloginformatico.com/

http://www.textoscientificos.com/

http://jemarinoi.googlepages.com/

http://www.delitosinformaticos.com/

http://seguridadsegura.blogspot.com/

http://www.informatica-juridica.com/

http://christianhg2009.wordpress.com/

http://gabriel.verdejo.alvarez.googlepages.com/

http://dmi.uib.es/

http://www.uv.es/

http://www.idg.es/

http://it.aut.uah.es/

http://www.belt.es/

http://itil.osiatis.es/

http://www.upm.es/

http://www.terra.es/

http://cert.inteco.es/

http://www.onnet.es/

http://www.dte.us.es/

http://www.unizar.es/

http://www.rediris.es/

http://www.a3m.eu/es/

http://lattice.ft.uam.es/

http://www.iec.csic.es/

http://www.lcc.uma.es/

http://integrity.abast.es/

http://www.it.uniovi.es/

http://www.emsisoft.es/

http://gsyc.escet.urjc.es/

http://www.elmundo.es/

http://pisuerga.inf.ubu.es/

https://www.ccn-cert.cni.es/

http://www-gti.det.uvigo.es/

http://www.criptored.upm.es/

http://www.securityartwork.es/

http://es.kioskea.net/

http://multingles.net/

http://www.duiops.net/

http://www.eumed.net/

http://web.uservers.net/

http://www.hipertext.net/

http://elistas.egrupos.net/

http://cfievalladolid2.net/

http://www.slideshare.net/

http://www.trucosgratis.net/

http://www.trucoswindows.net/

http://www.proteccion-datos.net/

http://marcos-yerena.lacoctelera.net/

http://cs.uns.edu.ar/

http://exa.unne.edu.ar/

http://www.lcu.com.ar/

http://www.aike.com.ar/

http://www.arcert.gov.ar/

http://www.alegsa.com.ar/

http://www.ciudad.com.ar/

http://www.linux-cd.com.ar/

http://www.segu-info.com.ar/

http://cxo-community.com.ar/

http://www.dirinfo.unsl.edu.ar/

http://www.econ.unicen.edu.ar/

http://www.nocturnabsas.com.ar/

http://www.antivirusgratis.com.ar/

http://www.pergaminovirtual.com.ar/

http://web.mit.edu/

http://www.ohio.edu/

http://servidor.acis.org.co/

http://www.interlan.com.co/

http://vector.ucaldas.edu.co/

http://fccea.unicauca.edu.co/

http://www.udistrital.edu.co/

http://www.escuelaing.edu.co/

http://www.virtual.unal.edu.co/

http://www.bcn.cl/

http://www.udec.cl/

http://www.clcert.cl/

http://www.kpmg.cl/

http://www.ing.puc.cl/

http://www.elo.utfsm.cl/

http://portal.inf.utfsm.cl/

http://www.pue.udlap.mx/

http://www.tuobra.unam.mx/

http://www.revista.unam.mx/

http://www.cafeonline.com.mx/

http://prof.usb.ve/

http://www.ldc.usb.ve/

http://definicion.de/

http://e-articles.info/

http://www.ucb.edu.bo/

http://www.universia.pr/

http://www.cepeu.edu.py/

ANEXOS

Anexo I. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. TÍTULO II Principios de la Protección de Datos.

Artículo 9. Seguridad de los datos.

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Anexo II. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. TÍTULO VIII de las Medidas de Seguridad en el Tratamiento de Datos de Carácter Personal.

CAPÍTULO I. DISPOSICIONES GENERALES.

Artículo 79. Alcance.

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento.

Artículo 80. Niveles de seguridad.

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Artículo 81. Aplicación de los niveles de seguridad.

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a. Los relativos a la comisión de infracciones administrativas o penales.

b. Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c. Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d. Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e. Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f. Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a. Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b. Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c. Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a. Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b. Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Artículo 82. Encargado del tratamiento.

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.

Artículo 83. Prestaciones de servicios sin acceso a datos personales.

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Artículo 84. Delegación de autorizaciones.

Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

Artículo 85. Acceso a datos a través de redes de comunicaciones.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.

Artículo 86. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 87. Ficheros temporales o copias de trabajo de documentos.

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II. DEL DOCUMENTO DE SEGURIDAD.

Artículo 88. El documento de seguridad.

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a. Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b. Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c. Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d. Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e. Procedimiento de notificación, gestión y respuesta ante las incidencias.

f. Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g. Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a. La identificación del responsable o responsables de seguridad.

b. Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

CAPÍTULO III. MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS AUTOMATIZADOS.

SECCIÓN I. MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO.

Artículo 89. Funciones y obligaciones del personal.

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 90. Registro de incidencias.

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 92. Gestión de soportes y documentos.

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 94. Copias de respaldo y recuperación.

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

SECCIÓN II. MEDIDAS DE SEGURIDAD DE NIVEL MEDIO.

Artículo 95. Responsable de seguridad.

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Artículo 96. Auditoría.

1. A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 97. Gestión de soportes y documentos.

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 98. Identificación y autenticación.

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 99. Control de acceso físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 100. Registro de incidencias.

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

SECCIÓN III. MEDIDAS DE SEGURIDAD DE NIVEL ALTO.

Artículo 101. Gestión y distribución de soportes.

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 102. Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 103. Registro de accesos.

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a. Que el responsable del fichero o del tratamiento sea una persona física.

b. Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Artículo 104. Telecomunicaciones.

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Anexo III. Tablas de Preguntas y Respuestas con sus pesos asignados

CONTRASEÑAS		
1	**¿Es posible acceder al sistema sin contraseña?**	
	• Sí, se puede acceder a cualquier información contenida en el sistema	0
	• Sólo a determinados servicios que no implican riesgo alguno de acceder a información no permitida	1
	• No	5
2	**¿Los usuarios se identifican individualmente?**	
	• Sí	5
	• No	0
3	**¿Los usuarios del sistema cambian su contraseña facilitada por defecto?**	
	• Sí	5
	• No	0
	• A los usuarios no se les facilitan contraseñas por defecto	N/A
4	**¿Las contraseñas contienen mayúsculas, minúsculas, números y signos de puntuación?**	
	• Sí	5
	• No	0
5	**¿Las contraseñas tienen una longitud mínima de ocho caracteres?**	
	• Sí	5
	• No	0
6	**¿Los usuarios evitan el uso de nombres, teléfonos, fechas señaladas o secuencias lógicas cuando crean sus contraseñas?**	
	• Sí	5
	• No	0
7	**¿Los usuarios cambian sus contraseñas, al menos, una vez cada 30 días o cuando sospechan que sus contraseñas han dejado de ser confidenciales?**	

	• Sí	5
	• No	0
8	**¿Los usuarios utilizan la misma contraseña para varios sistemas?**	
	• Sí	0
	• No	5
	• Los usuarios sólo se identifican en un único sistema	N/A
9	**¿Los usuarios almacenan sus contraseñas en archivos, las escriben en un pósit o se las facilitan a terceros?**	
	• Sí	0
	• No	5
10	**¿Se comprueba que los usuarios no utilizan contraseñas ya usadas anteriormente?**	
	• Sí	5
	• No	0

DATOS PERSONALES		
1	**¿La creación de ficheros de titularidad privada que contienen datos de carácter personal se notifican a la Agencia Española de Protección de Datos?**	
	• Sí	5
	• No	0
2	**¿A todos los ficheros que contienen datos de carácter personal se les aplica, al menos, medidas de nivel básico?**	
	• Sí	5
	• No	0
	• La organización no maneja ficheros con datos personales, excepto tratamiento de personas jurídicas o ficheros que contienen datos de personas físicas que prestan sus servicios en aquéllas, incorporando únicamente su nombre y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, teléfono y número de fax profesionales.	N/A
3	**¿El responsable del fichero (y el encargado del tratamiento, en su caso) adoptan las medidas de índole técnica y organizativa para garantizar la seguridad de los datos de carácter personal y evitar la modificación, tratamiento o acceso a los datos sin autorización?**	
	• Sí	5
	• No	0
4	**¿Se hacen efectivos los derechos de acceso, rectificación, cancelación y oposición a los individuos de los que se almacenan datos personales de la manera y en los tiempos establecidos en la Ley Orgánica 15/1999 de protección de datos de carácter personal (LOPD)?**	
	• Sí	5
	• No	0
5	**¿Los datos de carácter personal mantenidos en ficheros que son incompletos o inexactos son cancelados y sustituidos en el plazo de 10 días desde que se conoce su inexactitud?**	
	• Sí	5
	• No	0
6	**¿Los datos personales mantenidos en ficheros son cancelados cuando han**	

	dejado de ser necesarios o pertinentes para el fin con el que se registraron?	
	• Sí	5
	• No	0
7	**Las personas de las que se almacenan datos de carácter personal en un fichero son informadas de:**	
	• La existencia del fichero o tratamiento, la finalidad de éste y los destinatarios	1
	• Los datos obligatorios y opcionales	1
	• Las consecuencias de facilitarlos o no hacerlo	1
	• Informar acerca del derecho a acceder, rectificar y cancelar sus datos	1
	• El responsable del tratamiento o su representante si aquél no se encuentra en territorio español	1
8	**¿Se solicita el consentimiento inequívoco del afectado para el tratamiento de sus datos personales?**	
	• Sí	5
	• No	0
	• No es necesario el consentimiento del afectado porque los datos se refieren a las partes de un contrato o precontrato de una relación laboral, administrativa o negocial.	N/A
9	**¿Las transferencias internacionales de datos de carácter personal se realizan a países que tienen un nivel de protección equiparable al que presta la ley (nivel marcado por la Agencia Española de Protección de Datos) o por las excepciones marcadas en la LOPD?**	
	• Sí	5
	• No	0
	• No se producen transferencias internacionales de datos de carácter personal	N/A
10	**¿Se aplican medidas de nivel medio en ficheros que contienen datos que permitan evaluar la personalidad o el comportamiento de los individuos y en el resto de los casos en que sea exigible?**	
	• Sí	5
	• No	0

	• No existen ficheros de tales características	N/A
11	**¿Se adoptan medidas pertinentes para evitar el acceso del personal no autorizado a datos personales, a los soportes donde se recogen o a los recursos del sistema de información?**	
	• Sí	5
	• No	0
12	**¿Elabora el responsable del fichero o tratamiento un documento de seguridad que recoge las medidas de índole técnica y organizativa, no contrarias a la normativa vigente, que cumple el personal con acceso a los sistemas de información?**	
	• Sí	5
	• No	0
13	**Seleccione los siguientes apartados contenidos en el documento de seguridad:**	
	• Ámbito de aplicación del documento de seguridad	1
	• Recursos protegidos	1
	• Normas, reglas, medidas, procedimientos de actuación y estándares necesarios para respaldar el nivel de seguridad que exige el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos	1
	• Funciones y obligaciones del personal con algún vínculo con el tratamiento de datos personales incorporados en los ficheros	1
	• Estructura de los ficheros que contienen datos de carácter personal	1
	• Descripción de los sistemas de información que manejan datos personales	1
	• Procedimientos ante incidencias	1
	• Procedimientos de recuperación de datos	1
	• Procedimientos para la realización de copias de respaldo y de recuperación de los datos	1
	• Medidas adoptadas para transportar o destruir soportes y documentos	1
14	**Señale las medidas de seguridad aplicables a ficheros y tratamientos automatizados de datos personales de nivel BÁSICO:**	

	• Existe un registro de incidencias	1
	• Control de accesos y la existencia de una lista actualizada con los accesos autorizados	1
	• Respaldo semanal, como mínimo, salvo que no existan modificaciones	1
	• Se verifican cada seis meses los mecanismos y procedimientos de recuperación y respaldo	1
	• No se realizan pruebas con datos reales, salvo que se realice una copia de seguridad anteriormente y se asegure un nivel de seguridad	1
15	**Marque las medidas de seguridad aplicables a fichero y tratamientos automatizados de datos personales de nivel MEDIO:**	
	• Identificación del responsable o responsables de seguridad	1
	• Realización de auditorías internas o externas cada dos años o siempre que se produzcan cambios importantes	1
	• Se limita el número de reintentos de acceso	1
	• Se establece un sistema de registro de entrada y otro de salida de soportes para conocer el tipo de documento o soporte, quién lo emite y quién lo recibe, fecha y hora, el número de documentos o soportes que se envían, el tipo de información y la forma de envío	1
	• Además del registro de incidencias, se indican los procedimientos de recuperación de datos	1
16	**Seleccione las medidas de seguridad aplicables a ficheros y tratamientos automatizados de datos personales de nivel ALTO:**	
	• Para la distribución de soportes que contienen datos personales se cifran dichos datos o se utiliza otro mecanismo que garantice que aquéllos no sean accesibles o manipulados durante su transporte; también se cifran los datos que contienen los dispositivos portátiles cuando éstos se encuentran fuera de las instalaciones	1
	• Se conserva una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de los equipos informáticos que los tratan	1
	• De cada intento de acceso se almacena: la identificación del usuario, fecha y hora, fichero al que se accede, tipo de acceso y si ha sido autorizado o denegado; y estos datos del registro de accesos se guardan, al menos, dos años. O bien esto se no aplica debido a que el responsable del fichero o del tratamiento es una	1

	persona física o garantiza que únicamente él tiene acceso y trata los datos personales	
	• El responsable de seguridad revisa, al menos, una vez al mes la información de control registrada y elabora un informe de las revisiones y los problemas detectados. O bien esto se no aplica debido a que el responsable del fichero o del tratamiento es una persona física o garantiza que únicamente él tiene acceso y trata los datos personales	1
	• La transmisión de datos por redes públicas o redes inalámbricas de comunicaciones electrónicas se realizan cifrando los datos o utilizando otro mecanismo que garantice que la información no se manipula por terceros ni sea inteligible	1

POLÍTICA DE SEGURIDAD		
1	**¿Se ha definido una política de seguridad en la organización?**	
	• Sí	5
	• No	0
	Si la respuesta es "no" las siguientes preguntas sobre políticas de seguridad no se formulan.	
2	**¿La política de seguridad es coherente con la política de la organización?**	
	• Sí	5
	• No	0
3	**¿La política de seguridad es conforme con los requisitos legales?**	
	• Sí	5
	• No	0
4	**¿La política de seguridad muestra un lenguaje entendible por todo el personal de la empresa?**	
	• Sí	5
	• No	0
5	**¿Se fomenta la comunicación de la política de seguridad?**	
	• Sí	5
	• No	0
6	**¿La política de seguridad se cumple rigurosamente por todos los empleados de la organización?**	
	• Sí	5
	• No	0
7	**¿La política se revisa y se actualiza con cierta periodicidad o si se produce algún cambio importante?**	
	• Sí	5
	• No	0
8	**¿Existe en la empresa un responsable o responsables encargados del desarrollo,**	

	revisión y evaluación de la Política de Seguridad con la suficiente formación y experiencia?	
	• Sí	5
	• No	0

CONTROL DE ACCESO LÓGICO		
1	**¿Existen controles de acceso lógicos a los sistemas de información?**	
	• Sí	5
	• No	0
	Si la respuesta es "no" el cuestionario sobre controles de acceso lógicos finaliza.	
2	**¿Se limita el número de intentos fallidos para la autenticación en el sistema?**	
	• Sí	5
	• No	0
3	**¿Existe una lista actualizada con los accesos autorizados?**	
	• Sí	5
	• No	0
4	**¿Existen ficheros de logs que registran los accesos a los recursos y los intentos de acceso no autorizados?**	
	• Sí	5
	• No	0
5	**¿Se producen revisiones periódicas de los controles de acceso lógicos a los datos?**	
	• Sí	5
	• No	0
6	**¿Los usuarios tienen acceso únicamente a los recursos que necesitan para desempeñar su labor?**	
	• Sí	5
	• No	0
7	**¿Se educa a los usuarios para que utilicen de manera adecuada los mecanismos de acceso a los sistemas de información?**	
	• Sí	5
	• No	0

8	**¿Se revocan los derechos de acceso al sistema cuando los usuarios finalizan su actividad en la empresa?**	
	• Sí	5
	• No	0

COPIAS DE SEGURIDAD		
1	**¿La organización realiza copias de seguridad?**	
	• Sí	5
	• No	0
	Si la respuesta es "no" el cuestionario sobre copias de seguridad finaliza.	
2	**¿Los empleados de la entidad son conscientes de la importancia de realizar copias de seguridad, el tipo de copias a realizar en cada circunstancia y la frecuencia de realización de las mismas es crucial para la operación continua de la organización?**	
	• Sí	5
	• No	0
3	**¿Las copias de seguridad garantizan la recuperación y la continuidad de toda la información relevante de la empresa sin interrumpir la actividad del sistema?**	
	• Sí, es posible realizar un backup sin necesidad de detener la labor del sistema	5
	• Para realizar copias de seguridad es necesario interrumpir la actividad del sistema	0
4	**¿Existe un responsable en el caso de que produzca un fallo en el procedimiento de respaldo?**	
	• Si	5
	• No	0
5	**¿Se ha restaurado alguna copia de seguridad y el proceso ha sido satisfactorio?**	
	• Sí	5
	• Se ha restaurado alguna copia pero el proceso no ha finalizado con éxito	1
	• No se ha probado a restaurar ninguna copia de seguridad	0
6	**¿Los procedimientos de respaldo automatizados son probados con suficiente antelación a su implementación y, más tarde, a intervalos regulares?**	
	• Sí	5
	• No	0

	• La entidad no utiliza procedimientos de respaldo automatizados	N/A
7	**¿Las copias de seguridad que contienen información confidencial son protegidas por mecanismos de cifrado?**	
	• Sí	5
	• No	0
8	**¿Se realizan copias de seguridad completas, al menos, una vez a la semana?**	
	• Sí	5
	• No	0

AMENAZAS LÓGICAS		
1	**¿Se han infectado en alguna ocasión, los equipos de la empresa con código malicioso?**	
	• No	5
	• Sí pero los programas antivirus lo detectaron y eliminaron antes de causar algún daño en la empresa	1
	• Sí	0
2	**¿Se utilizan programas antivirus para prevenir, detectar y eliminar malware?**	
	• Si	5
	• No	0
3	**Marque los tipos de ataque que se ha sufrido la organización:**	
	• Ataque de autenticación	0 Marcado (1 sin marcar)
	• Ataque de denegación de servicio	0 Marcado (1 sin marcar)
	• Ataque de modificación	0 Marcado (1 sin marcar)
	• Ataque de intercepción	0 Marcado (1 sin marcar)
4	**¿Se utilizan técnicas de cifrado para salvaguardar la confidencialidad de la información si se produjera un ataque de intercepción?**	
	• Si	5
	• No	0
5	**¿Se utiliza un cortafuegos bien configurado para actuar como filtro entre redes facilitando las comunicaciones autorizadas y evitando los accesos ilícitos?**	

	• Si	5
	• No	0
6	**¿Se forma a los empleados para evitar los ataques, especialmente los de ingeniería social?**	
	• Si	5
	• No	0
7	**¿Se realizan pruebas para verificar que los mecanismos de seguridad funcionan correctamente?**	
	• Si	5
	• No	0

PROGRAMAS		
1	**¿Los programas instalados en los equipos de la entidad utilizan programas originales?**	
	• Sí	5
	• No	0
2	**¿Los empleados tienen restringido los programas a los que pueden acceder para realizar su actividad dentro de la compañía?**	
	• Sí	5
	• No	0
3	**¿Se instalan los parches y las últimas versiones de los programas usados en la organización?**	
	• Sí	5
	• No	0
4	**¿Los empleados ejecutan programas de origen desconocido?**	
	• Sí	0
	• No	5
5	**¿Se actualizan con frecuencia los programas dedicados a la detección y eliminación de código malicioso?**	
	• Sí	5
	• No	1
	• La entidad no utiliza programas dedicados a dicho fin	0

Anexo IV. Tablas de Preguntas y Respuestas con sus recomendaciones

CONTRASEÑAS		
1	**¿Es posible acceder al sistema sin contraseña?**	
	• Sí, se puede acceder a cualquier información contenida en el sistema	0
	RECOMENDACIÓN: Se debería acceder al sistema con una contraseña.	
	• Sólo a determinados servicios que no implican riesgo alguno de acceder a información no permitida	1
	RECOMENDACIÓN: Sería conveniente que los usuarios accedieran al sistema siempre a través de un identificador y una contraseña.	
2	**¿Los usuarios se identifican individualmente?**	
	• No	0
	RECOMENDACIÓN: Es muy recomendable que los usuarios posean un identificador y contraseña individual.	
3	**¿Los usuarios del sistema cambian su contraseña facilitada por defecto?**	
	• No	0
	RECOMENDACIÓN: Los usuarios deberían cambiar la contraseña recibida por defecto en cuanto les sea facilitada.	
4	**¿Las contraseñas contienen mayúsculas, minúsculas, números y signos de puntuación?**	
	• No	0
	RECOMENDACIÓN: Es importante que las contraseñas sean difíciles de 'adivinar' por lo que deben estar formadas por mayúsculas, minúsculas, números y signos de puntuación.	
5	**¿Las contraseñas tienen una longitud mínima de ocho caracteres?**	
	• No	0
	RECOMENDACIÓN: Conviene que la contraseña tenga una longitud de, al menos, ocho caracteres para que sea difícil de averiguar.	
6	**¿Los usuarios evitan el uso de nombres, teléfonos, fechas señaladas o secuencias lógicas cuando crean sus contraseñas?**	

	• No	0
	RECOMENDACIÓN: No es recomendable la utilización de secuencias lógicas, nombre, fechas, etc. porque facilitan que otras personas puedan adivinar la contraseña.	
7	**¿Los usuarios cambian sus contraseñas, al menos, una vez cada 30 días o cuando sospechan que sus contraseñas han dejado de ser confidenciales?**	
	• No	0
	RECOMENDACIÓN: Las contraseñas deben cambiarse cada 30 días o cuando el usuario sospeche que ha perdido su propiedad de confidencialidad.	
8	**¿Los usuarios utilizan la misma contraseña para varios sistemas?**	
	• Sí	0
	RECOMENDACIÓN: Es conveniente no utilizar la misma contraseña en varios sistemas porque si otra persona averigua la contraseña tendrá acceso a todos los sistemas en los que el usuario se identifica con ésta.	
9	**¿Los usuarios almacenan sus contraseñas en archivos, las escriben en un pósit o se las facilitan a terceros?**	
	• Sí	0
	RECOMENDACIÓN: Para conservar la propiedad de confidencialidad, las contraseñas no deben ser facilitadas a otras personas, ni ser escritas en ningún documento al cual puedan acceder individuos distintos del usuario.	
10	**¿Se comprueba que los usuarios no utilizan contraseñas ya usadas anteriormente?**	
	• No	0
	RECOMENDACIÓN: Se recomienda que los usuarios no puedan utilizar contraseñas que ya utilizaron antiguamente para acceder al sistema.	

DATOS PERSONALES		
1	**¿La creación de ficheros de titularidad privada que contienen datos de carácter personal se notifican a la Agencia Española de Protección de Datos?**	
	• No	0
	RECOMENDACIÓN: Todos los ficheros de titularidad privada que contengan datos de carácter personal deben notificarse a la Agencia Española de Protección de datos debido a que si no se notifican, se está incurriendo en una infracción grave según los artículos 26. 1 y 44. 3. i) de la Ley Orgánica 15/1999.	
2	**¿A todos los ficheros que contienen datos de carácter personal se les aplica, al menos, medidas de nivel básico?**	
	• No	0
	RECOMENDACIÓN: A todos los ficheros o tratamientos de datos personales se les debe aplicar las medidas de seguridad de nivel básico según el artículo 81. 1 del Título VIII del Real Decreto 1720/2007.	
3	**¿El responsable del fichero (y el encargado del tratamiento, en su caso) adoptan las medidas de índole técnica y organizativa para garantizar la seguridad de los datos de carácter personal y evitar la modificación, tratamiento o acceso a los datos sin autorización?**	
	• No	0
	RECOMENDACIÓN: El responsable del fichero (y el encargado del tratamiento, en su caso) debe adoptar las medidas de índole técnica y organizativa para garantizar la seguridad de los datos personales y así evitar su modificación, pérdida, acceso o tratamiento no autorizado, según el artículo 9 de la Ley Orgánica de Protección de Datos.	
4	**¿Se hacen efectivos los derechos de acceso, rectificación, cancelación y oposición a los individuos de los que se almacenan datos personales de la manera y en los tiempos establecidos en la Ley Orgánica 15/1999 de protección de datos de carácter personal (LOPD)?**	
	• No	0
	RECOMENDACIÓN: Los individuos de los que se almacenen datos de carácter personal tienen el derecho de acceso, rectificación, cancelación y oposición (entre otros derechos) de los datos recogidos. La negativa a facilitarle estos derechos contemplados en los artículos 15, 16, 17 y 18 de la L.O.P.D puede incurrir en sanciones debido a su carácter de infracción leve, grave o muy grave (dependiendo del tipo de infracción cometida reflejadas en el artículo 44 de dicha ley).	

5	**¿Los datos de carácter personal mantenidos en ficheros que son incompletos o inexactos son cancelados y sustituidos en el plazo de 10 días desde que se conoce su inexactitud?**	
	• No	0
	RECOMENDACIÓN: Los datos que no sean exactos y puestos al día deben ser cancelados y sustituidos por los correctos, en el plazo de 10 días desde que se tiene conocimiento de dicha inexactitud. En el caso de que los datos hayan sido comunicados a un cesionario, el plazo para comunicarle la inexactitud de aquéllos será de 10 días, y el cesionario contará con el mismo periodo de tiempo para cancelar y sustituir tales datos, según el artículo 4. 3 de la Ley Orgánica 15/1999.	
6	**¿Los datos personales mantenidos en ficheros son cancelados cuando han dejado de ser necesarios o pertinentes para el fin con el que se registraron?**	
	• No	0
	RECOMENDACIÓN: Los datos de carácter personal deben ser cancelados cuando ya no sean necesarios o pertinentes para el fin con el que se recogieron o registraron, según el artículo 4. 5 de la Ley Orgánica de Protección de Datos.	
7	**Las personas de las que se almacenan datos de carácter personal en un fichero son informadas de:**	
	• La existencia del fichero o tratamiento, la finalidad de éste y los destinatarios	Sin marcar 0
	• Los datos obligatorios y opcionales	Sin marcar 0
	• Las consecuencias de facilitarlos o no hacerlo	Sin marcar 0
	• Informar acerca del derecho a acceder, rectificar y cancelar sus datos	Sin marcar 0
	• El responsable del tratamiento o su representante si aquél no se encuentra en territorio español	Sin marcar 0
	RECOMENDACIÓN: Es importante que se informe a las personas de las que se recaba datos de carácter personal de: (si la primera opción de las respuestas no está marcada) la existencia del fichero o tratamiento, la finalidad de éste y los destinatarios; (2ª opción no marcada) cuales son	

	datos obligatorios y cuales opcionales; (3ª opción no marcada) las consecuencias de facilitar los datos personales o de no hacerlo; (4ª opción no marcada) informar del derecho a acceder, rectificar y cancelar los datos de carácter personal; (5ª opción no marcada) la identidad del responsable del tratamiento o su representante si aquél no se encuentra en territorio español.	
8	**¿Se solicita el consentimiento inequívoco del afectado para el tratamiento de sus datos personales?**	
	• No	0
	RECOMENDACIÓN: Es necesario el consentimiento del afectado para el tratamiento de sus datos personales excepto en los casos especificados en el artículo 6. 2 de la LOPD.	
9	**¿Las transferencias internacionales de datos de carácter personal se realizan a países que tienen un nivel de protección equiparable al que presta la ley (nivel marcado por la Agencia Española de Protección de Datos) o por las excepciones marcadas en la LOPD?**	
	• No	0
	RECOMENDACIÓN: No se ha de realizar transferencias internacionales de datos de carácter personal a países con un nivel de protección menor al que presta la ley, salvo autorización previa del director de la Agencia Española de Protección de Datos o las excepciones marcadas en el artículo 34 de la Ley Orgánica 15/1999.	
10	**¿Se aplican medidas de nivel medio en ficheros que contienen datos que permitan evaluar la personalidad o el comportamiento de los individuos y en el resto de los casos en que sea exigible?**	
	• No	0
	RECOMENDACIÓN: Es necesario aplicar medidas de nivel medio a ficheros que contengan datos que permitan evaluar la personalidad o el comportamiento de los individuos, según el artículo 81. 2. f del Título VIII del Real Decreto 1720/2007.	
11	**¿Se adoptan medidas pertinentes para evitar el acceso del personal no autorizado a datos personales, a los soportes donde se recogen o a los recursos del sistema de información?**	
	• No	0
	RECOMENDACIÓN: El responsable del fichero o del tratamiento debe adoptar las medidas para limitar el acceso a datos de carácter personal por parte del personal. Este requerimiento está recogido en el artículo 83 del Reglamento de desarrollo de la LOPD.	

12	**¿Elabora el responsable del fichero o tratamiento un documento de seguridad que recoge las medidas de índole técnica y organizativa, no contrarias a la normativa vigente, que cumple el personal con acceso a los sistemas de información?**	
	• No	0
	RECOMENDACIÓN: El responsable del fichero o tratamiento debe elaborar un documento de seguridad que recoja las medidas de índole técnica y organizativa, que será de riguroso cumplimiento por todo el personal con acceso a los sistemas, según el artículo 88 del Real Decreto 1720/2007.	
13	**Seleccione los siguientes apartados contenidos en el documento de seguridad:**	
	• Ámbito de aplicación del documento de seguridad	Sin marcar 0
	• Recursos protegidos	Sin marcar 0
	• Normas, reglas, medidas, procedimientos de actuación y estándares necesarios para respaldar el nivel de seguridad que exige el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos	Sin marcar 0
	• Funciones y obligaciones del personal con algún vínculo con el tratamiento de datos personales incorporados en los ficheros	Sin marcar 0
	• Estructura de los ficheros que contienen datos de carácter personal	Sin marcar 0
	• Descripción de los sistemas de información que manejan datos personales	Sin marcar 0
	• Procedimientos ante incidencias	Sin marcar 0
	• Procedimientos de recuperación de datos	Sin marcar 0
	• Procedimientos para la realización de de copias de respaldo y de recuperación de los datos	Sin marcar

		0
	• Medidas adoptadas para transportar o destruir soportes y documentos	Sin marcar 0
	RECOMENDACIÓN: El documento de seguridad debe contener: (si la primera opción de las respuestas no está marcada) el ámbito de aplicación del documento; (2ª opción no marcada) los recursos protegidos por éste; (3ª opción no marcada) las normas, reglas, medidas, procedimientos de actuación y estándares necesarios para respaldar el nivel de seguridad que exige el Real Decreto 1720/2007; (4ª opción no marcada)las obligaciones y las funciones del personal relacionados con los datos personales incorporados en los ficheros; (5ª opción no marcada) la estructura de los ficheros que almacenan datos de carácter personal; (6ª opción no marcada) la descripción de los sistemas de información que utilizan datos personales; (7ª opción no marcada) los procedimientos de comunicación, gestión y respuesta ante incidencias; (8ª opción no marcada) los procedimientos de recuperación de datos en los ficheros o tratamientos; (9ª opción no marcada) los procedimientos para llevar a cabo las copias de respaldo y de recuperación de los datos; (10ª opción no marcada) las medidas que se adoptan para el transporte de soportes y documentos y las medidas necesarias para su destrucción.	
14	**Señale las medidas de seguridad aplicables a ficheros y tratamientos automatizados de datos personales de nivel BÁSICO:**	
	• Existe un registro de incidencias	Sin marcar 0
	• Control de accesos y la existencia de una lista actualizada con los accesos autorizados	Sin marcar 0
	• Respaldo semanal, como mínimo, salvo que no existan modificaciones	Sin marcar 0
	• Se verifican cada seis meses los mecanismos y procedimientos de recuperación y respaldo	Sin marcar 0
	• No se realizan pruebas con datos reales, salvo que se realice una copia de seguridad anteriormente y se asegure un nivel de seguridad	Sin marcar 0
	RECOMENDACIÓN: Se deben aplicar una serie de medidas de seguridad sobre ficheros y tratamiento de datos personales con nivel básico exigido, recomendaciones ampliadas en el capítulo III sección I del título VIII del Real Decreto 1720/2007: (si la primera opción de las	

	respuestas no está marcada) un registro de incidencias que afecten a los datos de carácter personal; (2ª opción no marcada) un control de acceso a los recursos y la existencia de una lista actualizada con los accesos autorizados; (3ª opción no marcada) se realiza un respaldo semanal, como mínimo, salvo si no se producen cambios; (4ª opción no marcada) se comprueban cada seis meses los procedimientos y mecanismos de respaldo y de recuperación; (5ª opción no marcada) no deben realizarse pruebas con datos reales, a menos que se garantice el nivel de seguridad y se realice una copia de seguridad.	
15	**Marque las medidas de seguridad aplicables a fichero y tratamientos automatizados de datos personales de nivel MEDIO:**	
	• Identificación del responsable o responsables de seguridad	Sin marcar 0
	• Realización de auditorías internas o externas cada dos años o siempre que se produzcan cambios importantes	Sin marcar 0
	• Se limita el número de intentos de acceso al sistema de información	Sin marcar 0
	• Se establece un sistema de registro de entrada y otro de salida de soportes para conocer el tipo de documento o soporte, quién lo emite y quién lo recibe, fecha y hora, el número de documentos o soportes que se envían, el tipo de información y la forma de envío	Sin marcar 0
	• Además del registro de incidencias, se indican los procedimientos de recuperación de datos	Sin marcar 0
	RECOMENDACIÓN: Además de aplicar las medidas de seguridad de nivel básico, se deben aplicar también medidas de seguridad sobre ficheros y tratamiento de datos personales con nivel medio exigido, recomendaciones ampliadas en el capítulo III sección II del título VIII del Real Decreto 1720/2007: (si la primera opción de las respuestas no está marcada) nombrar un responsable de seguridad; (2ª opción no marcada) realizar auditorías cada dos años o si se producen cambios significativos; (3ª opción no marcada) limitar los intentos al sistema de información; (4ª opción no marcada) establecer un sistema de registro de entrada de soportes; (5ª opción no marcada) indicar los procedimientos de recuperación de datos.	
16	**Seleccione las medidas de seguridad aplicables a ficheros y tratamientos automatizados de datos personales de nivel ALTO:**	
	• Para la distribución de soportes que contienen datos personales se cifran dichos datos o se utiliza otro mecanismo que garantice que	Sin marcar

aquéllos no sean accesibles o manipulados durante su transporte; también se cifran los datos que contienen los dispositivos portátiles cuando éstos se encuentran fuera de las instalaciones	0
• Se conserva una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de los equipos informáticos que los tratan	Sin marcar 0
• De cada intento de acceso se almacena: la identificación del usuario, fecha y hora, fichero al que se accede, tipo de acceso y si ha sido autorizado o denegado; y estos datos del registro de accesos se guardan, al menos, dos años. O bien esto se no aplica debido a que el responsable del fichero o del tratamiento es una persona física o garantiza que únicamente él tiene acceso y trata los datos personales	Sin marcar 0
• El responsable de seguridad revisa, al menos, una vez al mes la información de control registrada y elabora un informe de las revisiones y los problemas detectados. O bien esto se no aplica debido a que el responsable del fichero o del tratamiento es una persona física o garantiza que únicamente él tiene acceso y trata los datos personales	Sin marcar 0
• La transmisión de datos por redes públicas o redes inalámbricas de comunicaciones electrónicas se realizan cifrando los datos o utilizando otro mecanismo que garantice que la información no se manipula por terceros ni sea inteligible	Sin marcar 0
RECOMENDACIÓN: Además de aplicar las medidas de seguridad de nivel medio, se han de aplicar las siguientes medidas de seguridad sobre ficheros y tratamiento de datos personales con nivel alto exigido, recomendaciones ampliadas en el capítulo III sección III del título VIII del Real Decreto 1720/2007: (1ª opción no marcada) cifrar los datos o usar otro mecanismo que garantice que éstos no sean accesibles o manipulados durante su transporte en la distribución de soportes que contienen datos de carácter personal , y cifrar los datos que contienen los dispositivos portátiles cuando no se encuentran en las instalaciones; (2ª opción no marcada) se debe conservar una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de los equipos informáticos que los tratan; (3ª opción no marcada) si el responsable del fichero o del tratamiento no es una persona física o no puede garantizar que sea el único que tiene acceso y trata los datos personales, debe guardar de cada intento de acceso: la identificación del usuario, fecha y hora, fichero accedido, tipo de acceso y si ha sido autorizado o denegado; y estos datos del registro de accesos se almacenan, al menos, dos años; (4ª opción no marcada) si el responsable del fichero o del tratamiento no es una persona física o no puede garantizar que sea el único que tiene acceso y trata los datos personales, el responsable de seguridad debe revisar, al menos, una vez al mes la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados; (5ª opción no marcada) cifrar los datos o utilizar	

	otro mecanismo que garantice que la información no se manipule por terceros ni sea inteligible en la transmisión de datos por redes públicas o redes inalámbricas de comunicaciones electrónicas.	

POLÍTICA DE SEGURIDAD		
1	**¿Se ha definido una política de seguridad en la organización?**	
	• No	0
	RECOMENDACIÓN: La organización debe redactar un documento que contenga la política de seguridad para regular el modo en el que los bienes que manejen información sensible son protegidos, gestionados y distribuidos. Por este motivo, no es posible continuar con el cuestionario sobre políticas de seguridad.	
2	**¿La política de seguridad es coherente con la política de la organización?**	
	• No	0
	RECOMENDACIÓN: Es necesario que la política de seguridad sea acorde a la política de la entidad.	
3	**¿La política de seguridad es conforme con los requisitos legales?**	
	• No	0
	RECOMENDACIÓN: Es imprescindible que la política de seguridad sea conforme a las normas legales vigentes.	
4	**¿La política de seguridad muestra un lenguaje entendible por todo el personal de la empresa?**	
	• No	0
	RECOMENDACIÓN: La política debe utilizar un lenguaje sencillo para su comprensión por todos los empleados de la empresa.	
5	**¿Se fomenta la comunicación de la política de seguridad?**	
	• No	0
	RECOMENDACIÓN: La política debe difundirse a toda la organización para conocerla, entenderla y cumplirla.	
6	**¿La política de seguridad se cumple rigurosamente por todos los empleados de la organización?**	
	• No	0
	RECOMENDACIÓN: Todos los empleados de la entidad deben cumplir la política de seguridad.	
7	**¿La política se revisa y se actualiza con cierta periodicidad o si se produce algún cambio importante?**	

	• No	0
	RECOMENDACIÓN: Es necesario que la política sea revisada y actualizada con cierta frecuencia o cuando sucede alguna modificación relevante.	
8	**¿Existe en la empresa un responsable o responsables encargados del desarrollo, revisión y evaluación de la política de seguridad con la suficiente formación y experiencia?**	
	• No	0
	RECOMENDACIÓN: En la organización debe existir un responsable (o responsables) que revise y actualice la política de seguridad. Además, tiene que contar con la formación y experiencia necesaria para realizar esa labor.	

CONTROL DE ACCESO LÓGICO		
1	**¿Existen controles de acceso lógicos a los sistemas de información?**	
	• No	0
	RECOMENDACIÓN: La organización debe implantar controles de acceso lógicos a los sistemas de información para evitar accesos no autorizados. Por lo tanto, no es posible continuar con el cuestionario sobre controles de acceso lógicos.	
2	**¿Se limita el número de intentos fallidos para la autenticación en el sistema?**	
	• No	0
	RECOMENDACIÓN: Es recomendable limitar el número de intentos fallidos de accesos al sistema y evitar así que personas no autorizadas traten de acceder al sistema ilimitadamente.	
3	**¿Existe una lista actualizada con los accesos autorizados?**	
	• No	0
	RECOMENDACIÓN: Se debe mantener una lista que contenga los accesos autorizados al sistema de información. Esta lista ha de estar actualizada para que usuarios a los que se les revoque el derecho de acceso, no puedan penetrar en dicho sistema.	
4	**¿Existen ficheros de logs que registran los accesos a los recursos y los intentos de acceso no autorizados?**	
	• No	0
	RECOMENDACIÓN: Es necesario que existan ficheros de logs para almacenar información de los accesos y los intentos de accesos no autorizados.	
5	**¿Se producen revisiones periódicas de los controles de acceso lógicos a los datos?**	
	• No	0
	RECOMENDACIÓN: Se recomienda realizar revisiones periódicas para asegurar que los controles de acceso funcionan según lo previsto.	
6	**¿Los usuarios tienen acceso únicamente a los recursos que necesitan para desempeñar su labor?**	
	• No	0
	RECOMENDACIÓN: Los usuarios deben disfrutar del mínimo	

	privilegio que necesiten para realizar su actividad dentro de la organización.	
7	**¿Se educa a los usuarios para que utilicen de manera adecuada los mecanismos de acceso a los sistemas de información?**	
	• No	0
	RECOMENDACIÓN: Es necesario instruir a los usuarios para que hagan un uso apropiado de los controles de acceso a los sistemas de información.	
8	**¿Se revocan los derechos de acceso al sistema cuando los usuarios finalizan su actividad en la empresa?**	
	• No	0
	RECOMENDACIÓN: Se deben revocar inmediatamente los derechos de acceso al sistema cuando un usuario deja de prestar servicio a la empresa.	

COPIAS DE SEGURIDAD		
1	**¿La organización realiza copias de seguridad?**	
	• No	0
	RECOMENDACIÓN: Para asegurar la continuidad del negocio, es necesario realizar copias de respaldo de la información contenida en la organización. Por lo tanto, no es posible continuar con el cuestionario sobre copias de seguridad.	
2	**¿Los empleados de la entidad son conscientes de la importancia de realizar copias de seguridad, el tipo de copias a realizar en cada circunstancia y la frecuencia de realización de las mismas es crucial para la operación continua de la organización?**	
	• No	0
	RECOMENDACIÓN: Es necesario que los empleados de la organización entiendan la importancia de realizar copias de seguridad para salvaguardar la información, el tipo de copias que se deben efectuar en cada ocasión y la frecuencia de realización según la criticidad de la información. El no tener presente estos aspectos, aboca a la empresa a una situación de riesgo.	
3	**¿Las copias de seguridad garantizan la recuperación y la continuidad de toda la información relevante de la empresa sin interrumpir la actividad del sistema?**	
	• Para realizar las copias de seguridad es necesario interrumpir la actividad del sistema	0
	RECOMENDACIÓN: Es recomendable que se puedan realizar copias de seguridad sin interrumpir la actividad del sistema, sobre todo, en sistemas con disponibilidad 24x7.	
4	**¿Existe un responsable en el caso de que produzca un fallo en el procedimiento de respaldo?**	
	• No	0
	RECOMENDACIÓN: Se debería designar un responsable o responsables que intervengan en el caso de que se produzca un fallo mientras se realiza una copia de seguridad.	
5	**¿Se ha restaurado alguna copia de seguridad y el proceso ha sido satisfactorio?**	
	• Se ha restaurado alguna copia pero el proceso no ha finalizado con éxito	1

	RECOMENDACIÓN: La organización ha restaurado copias de seguridad pero es necesario que el procedimiento finalice con éxito.	
	• No se ha probado a restaurar ninguna copia de seguridad.	0
	RECOMENDACIÓN: Es conveniente restaurar alguna copia de seguridad para cerciorarse que dicha restauración se lleva a cabo de forma adecuada.	
6	**¿Los procedimientos de respaldo automatizados son probados con suficiente antelación a su implementación y, más tarde, a intervalos regulares?**	
	• No	0
	RECOMENDACIÓN: Para cerciorarse de que los procedimientos de respaldo automatizados funcionan correctamente antes de su implantación, es necesario realizar una serie de pruebas que aseguren que aquéllos funcionan con normalidad. Además, se deben realizar pruebas periódicamente durante el proceso de mantenimiento para constatar que su comportamiento es el adecuado.	
7	**¿Las copias de seguridad que contienen información confidencial son protegidas por mecanismos de cifrado?**	
	• No	0
	RECOMENDACIÓN: Las copias de seguridad que contengan información confidencial deben utilizar mecanismos de cifrado para evitar que personas no autorizadas puedan conocer el contenido de dicha información.	
8	**¿Se realizan copias de seguridad completas, al menos, una vez a la semana?**	
	• No	0
	RECOMENDACIÓN: Las copias de seguridad completas se utilizan para salvaguardar toda la información de un fichero o ficheros que posee la organización. Este tipo de backups no tiene en cuenta que la información ya hubiera sido copiada, ocupan gran cantidad de dispositivos de almacenamiento pero la velocidad de recuperación es menor en comparación con otros tipos de copias de seguridad. Es importante realizar backups totales, al menos, semanalmente.	

AMENAZAS LÓGICAS		
1	**¿Se han infectado en alguna ocasión, los equipos de la empresa con código malicioso?**	
	• Sí pero los programas antivirus lo detectaron y eliminaron antes de causar algún daño en la empresa	1
	RECOMENDACIÓN: Aunque el daño no se ha materializado, es recomendable detectar cómo se infectaron los equipos con código malicioso y qué controles de seguridad fallaron.	
	• Sí	0
	RECOMENDACIÓN: Es necesario utilizar programas antivirus y otras herramientas encargadas de prevenir la infección de los ordenadores, además de detectar y eliminar virus y otras amenazas lógicas. Si se infectan los equipos informáticos se debe averiguar que controles de seguridad han fallado y poner remedio para que no vuelva a ocurrir.	
2	**¿Se utilizan programas antivirus para prevenir, detectar y eliminar malware?**	
	• No	0
	RECOMENDACIÓN: Es vital para salvaguardar los equipos, utilizar entre otros métodos de protección, programas antivirus para evitar que los equipos se infecten con código malicioso.	
3	**Marque los tipos de ataque que se ha sufrido la organización:**	
	• Ataque de autenticación	0 Marcado
	• Ataque de denegación de servicio	0 Marcado
	• Ataque de modificación	0 Marcado
	• Ataque de intercepción	0 Marcado
	RECOMENDACIÓN: Revisar los métodos de protección, en especial, los programas antivirus, cortafuegos, técnicas de cifrado y copias de seguridad para evitar que se produzcan nuevamente ataques lógicos.	
4	**¿Se utilizan técnicas de cifrado para salvaguardar la confidencialidad de la información si se produjera un ataque de intercepción?**	

	• No	0
	RECOMENDACIÓN: Si se ha producido un ataque de intercepción de la información, es muy recomendable cifrar la información confidencial.	
5	**¿Se utiliza un cortafuegos bien configurado para actuar como filtro entre redes facilitando las comunicaciones autorizadas y evitando los accesos ilícitos?**	
	• No	0
	RECOMENDACIÓN: El uso de cortafuegos evita accesos ilícitos a la red privada y permite el paso del tráfico autorizado a través de políticas de seguridad preestablecidas.	
6	**¿Se forma a los empleados para evitar los ataques, especialmente los de ingeniería social?**	
	No	0
	RECOMENDACIÓN: Es necesario ofrecer una formación a los empleados para que conozcan las amenazas lógicas a las que se enfrentan.	
7	**¿Se realizan pruebas para verificar que los mecanismos de seguridad funcionan correctamente?**	
	• No	0
	RECOMENDACIÓN: Se deben realizar pruebas para verificar que los controles de seguridad funcionan de forma adecuada.	

	PROGRAMAS	
1	**¿Los programas instalados en los equipos de la entidad utilizan programas originales?**	
	• No	0
	RECOMENDACIÓN: Se recomienda el uso de programas originales para evitar que contengan código malicioso que pueda dañar el sistema.	
2	**¿Los empleados tienen restringido los programas a los que pueden acceder para realizar su actividad dentro de la compañía?**	
	• No	0
	RECOMENDACIÓN: Los empleados no deben tener acceso a todos los programas de la organización para que no puedan producir un daño (accidental o intencionado). Sólo han de tener acceso a aquellos programas que sean necesarios para desempeñar su labor dentro de la compañía.	
3	**¿Se instalan los parches y las últimas versiones de los programas usados en la organización?**	
	• No	0
	RECOMENDACIÓN: Es necesario instalar los parches y las últimas versiones de los programas para corregir posibles errores y vulnerabilidades que presenten dichos programas.	
4	**¿Los empleados ejecutan programas de origen desconocido?**	
	• Si	0
	RECOMENDACIÓN: Se ha de evitar ejecutar programas de origen desconocido para que no supongan una amenaza lógica para la entidad.	
5	**¿Se actualizan con frecuencia los programas dedicados a la detección y eliminación de código malicioso?**	
	• No	1
	RECOMENDACIÓN: Deben actualizarse con frecuencia los programas dedicados a detectar y eliminar malware de los equipos de la entidad. En el caso de los antivirus, lo ideal es actualizarlos diariamente.	
	• La entidad no utiliza programas dedicados a dicho fin	0
	RECOMENDACIÓN: Es muy importante el uso de programas destinados a detectar y eliminar código malicioso de los ordenadores para que la organización esté a salvo de este tipo de amenazas.	